

Management Software

AT-S25



User's Guide

AT-8316F/MT, AT-8316F/VF, AT-8316F/SC, AND
AT-8324 FAST ETHERNET SWITCHES

VERSION 2.0.2

PN 613-10844-00 Rev E



Simply Connecting the  World

Copyright © 2003 Allied Telesyn, Inc.
960 Stewart Drive Suite B, Sunnyvale, CA 94085 USA

All rights reserved. No part of this publication may be reproduced without prior written permission from Allied Telesyn, Inc.

Microsoft is a registered trademark of Microsoft Corporation, Netscape Navigator is a registered trademark of Netscape Communications Corporation. All other product names, company names, logos or other designations mentioned herein are trademarks or registered trademarks of their respective owners.

Allied Telesyn, Inc. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesyn, Inc. be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein, even if Allied Telesyn, Inc. has been advised of, known, or should have known, the possibility of such damages.

Table of Contents

List of Figures	8
List of Tables	11
Preface	12
How This Guide is Organized	13
Document Conventions	14
Contacting Allied Telesyn	15
Online Support.....	15
E-mail and Telephone Support	15
For Sales or Corporate Information	15
Where to Find Web-based Guides	16
Obtaining Management Software Updates	16
Upgrading AT-S25 Version 1.5.6.2 or Earlier to Version 2.0.2 or Later	17
TFTP Guidelines.....	18
Using TFTP to Download the AT-S25 Version 2.0.2 Image File to the Master Switch of the Stack.....	19
Using XModem to Download the AT-S25 Version 2.0.2 Image File	19
 Section I	
Overview	25
Chapter 1	
Overview	26
Local Management Session	28
Telnet Management Session	29
Web Browser Management Session	30
SNMP Management Session	31
Management Access Levels	32
 Section II	
Local and Telnet Management Sessions	33
Chapter 2	
Starting a Local or Telnet Management Session	34
Local Management Session	35
Starting a Local Management Interface.....	35
Quitting from a Local Interface	37

Telnet Management Session	38
Starting a Telnet Management Interface	38
Quitting from a Telnet Management Interface	39
Selecting a Switch Module in the Stack	40
Chapter 3	
Basic Switch Parameters	41
When Does a Switch Need an IP Address?	42
How Do You Assign an IP Address?	42
Configuring an IP Address and Switch Name	45
Activating the BOOTP and DHCP Services	46
Resetting a Stack	48
Pinging a Remote System	49
Configuring the AT-S25 Software Security Features	50
Configuring the Management Passwords	51
Configuring Management Access	52
Configuring SNMP Community Strings and Trap IP Addresses	54
Returning the AT-S25 Software to the Factory Default Values	56
Viewing the AT-S25 Version Number and Basic Switch Information	58
Chapter 4	
Port Parameters	59
Configuring Port Parameters	60
Displaying Port Status	64
Chapter 5	
Port Security	67
Port Security Overview	68
Automatic	68
Limited	68
Secure	70
Lock All Ports	71
Configuring Limited Security Level	72
Activating a Port Security Level	75
Chapter 6	
Port Trunking	77
Port Trunking Overview	78
Port Trunking Guidelines	78
Creating a Port Trunk	82
Creating a 10/100 Port Trunk	82
Creating a Gigabit Port Trunk	83
Modifying a Port Trunk	85
Modifying a Trunk Name	86
Deleting a Port Trunk	87
Chapter 7	
Port Mirroring	88
Port Mirroring Overview	89
Creating a Port Mirror	90
Chapter 8	
STP and RSTP	92
STP and RSTP Overview	93
Bridge Priority and the Root Bridge	94
Mixed STP and RSTP Networks	100
Spanning Tree and VLANs	100

Enabling or Disabling STP or RSTP	101
STP and RSTP Parameters	102
Configuring STP	105
Configuring a Bridge's STP Settings	105
Configuring a Port's STP Settings	107
Displaying Port's STP Status and Setting	109
Configuring RSTP	110
Configuring a Bridge's RSTP Settings	110
Configuring a Port's RSTP Settings	111
Displaying Port's RSTP Status and Settings	114
Displaying a Port's RSTP Settings	114
Displaying a Port's RSTP Status	115

Chapter 9

Virtual LANs	117
VLAN Overview	118
Port-based VLAN Overview	120
VLAN Name	120
VLAN Identifier	120
Untagged Ports	121
Port VLAN Identifier	121
General Rules to Creating a Port-based VLAN	121
Drawbacks to Port-based VLANs	122
Port-based VLAN Example	123
Tagged VLAN Overview	125
VLAN Name	126
VLAN Identifier	126
Tagged and Untagged Ports	126
Port VLAN Identifier	126
General Rules to Creating a Tagged VLAN	126
Tagged VLAN Example	127
Basic VLAN Mode Overview	129
Creating a Port-based or Tagged VLAN	130
Modifying a VLAN	134
Displaying VLAN Information	137
Deleting a VLAN	138
Deleting All VLANs	140
Displaying PVIDs	141
Specifying a Management VLAN	143
Switching the VLAN Mode	145

Chapter 10

MAC Address Table	146
MAC Address Overview	147
Viewing MAC Addresses	149
Viewing All MAC Addresses	149
Viewing Static MAC Addresses Only	151
Viewing Multicast MAC Addresses Only	152
Viewing MAC Addresses on Base Ports Only	153
Viewing MAC Addresses by Port & Module	154
Viewing the MAC Addresses of a VLAN	155
Identifying a Port or a Module Number by MAC Address	156
Deleting MAC Addresses	157
Deleting All Dynamic MAC Addresses	158
Adding Static and Multicast MAC Addresses	159
Changing the Aging Time	160

Chapter 11

Class of Service	161
Class of Service Overview	162
Configuring CoS	163
Show Port VLANs & Priorities	165

Chapter 12

IGMP Snooping	166
IGMP Snooping Overview	167
Activating IGMP Snooping	169
Displaying a List of Host Nodes	172
Displaying a List of Multicast Routers	173

Chapter 13

Ethernet Statistics	174
Displaying Port Statistics	175
Displaying Switch Statistics	177

Chapter 14

File Downloads and Uploads	178
Obtaining Software Updates	180
Transferring Files from a Local Management Interface	181
Downloading An Image File	182
Downloading Configuration File.....	184
Uploading Configuration File to TFTP Server	185
Transferring Files Using HyperTerminal Interface	186

Section III**Web Browser Management** 188**Chapter 15**

Starting a Web Browser Management Interface	189
Web Browser Management Interface	190
Starting a Web Browser Interface	190
Browser Tools	192
Quitting from a Web Browser Management Interface.....	192

Chapter 16

Basic Switch Parameters	193
Configuring an IP Address and Switch Name	194
Activating the BOOTP and DHCP Services	198
Resetting a Switch	199
Viewing System Information	200
Configuring the SNMP Parameters and Trap IP Addresses	202
Pinging a Remote System	204
Returning the AT-S25 Software to the Factory Default Values	205

Chapter 17

Port Parameters	206
Configuring Port Parameters	207
Displaying Port Status and Statistics	210

Chapter 18

Port Security	214
Displaying the Port Security Level	215

Chapter 19	
Port Trunks	216
Creating a Port Trunk	217
Modifying a Port Trunk	219
Deleting a Port Trunk	220
Displaying Port Trunks	221
Chapter 20	
Port Mirroring	222
Creating a Port Mirror	223
Deleting a Port Mirror	225
Viewing Source and Destination Ports	226
Chapter 21	
STP and RSTP	227
Enabling or Disabling STP or RSTP	228
STP and RSTP Parameters	230
Configuring STP	233
Configuring a Bridge's STP Settings	233
Configuring a Port's STP Settings	234
Displaying STP Status and Settings	235
Displaying Bridge's STP Status and Settings	235
Displaying Port's STP Status and Settings	235
Configuring RSTP	237
Configuring a Bridge's RSTP Settings	237
Configuring a Port's RSTP Settings	238
Displaying RSTP Status and Settings	240
Displaying Bridge's RSTP Status and Settings	240
Displaying Port's RSTP Status and Settings	240
Chapter 22	
Virtual LANs	242
Creating a VLAN	243
Modifying a VLAN	245
Deleting VLANs	247
Displaying VLANs	248
Changing a PVID Value	250
Setting the Switch's VLAN Mode	252
Chapter 23	
MAC Address Table	254
Viewing the MAC Address Table	255
Adding Static and Multicast MAC Addresses	258
Deleting MAC Addresses	259
Changing the Aging Time	260
Chapter 24	
Class of Service	262
Configuring CoS	263
Chapter 25	
IGMP Snooping	265
Configuring IGMP Snooping	266
Displaying a List of Host Nodes and Multicast Routers	269
Appendix A	
AT-S25 Default Settings	272
Index	274

List of Figures

Figure 1:	System Booting Window	20
Figure 2:	ATI Diagnostics Menu	21
Figure 3:	AT-S25 Properties Window	22
Figure 4:	COM1 Properties Window	22
Figure 5:	Local Management Window - Send File Menu	23
Figure 6:	Send File Pop-Up Window	23
Figure 7:	XModem File Send Window	24
Figure 8:	Connecting a Terminal or PC to the RS-232 Terminal Port	35
Figure 9:	Main Menu	37
Figure 10:	Administration Menu	43
Figure 11:	Passwords Menu	51
Figure 12:	System Config Menu	52
Figure 13:	Advanced Configuration Menu	54
Figure 14:	SNMP Configuration Menu	55
Figure 15:	Diagnostics Menu	58
Figure 16:	Example of Port Configuration Menu	61
Figure 17:	Ports Menu	64
Figure 18:	Port Status Window	65
Figure 19:	Port Groupings on an AT-8324 Switch	69
Figure 20:	Port Groups on an AT-8316F/MT or AT-8316/VF Switch	69
Figure 21:	Port Groups on an AT-8316F/SC Switch	70
Figure 22:	Port Security Menu	72
Figure 23:	Port Security Limited-Mode Menu	73
Figure 24:	Port Security Menu	75
Figure 25:	Port Trunk Example	78
Figure 26:	Port Groupings on an AT-8324 Switch	79
Figure 27:	Port Groups on an AT-8316F/MT or AT-8316/VF Switch	79
Figure 28:	Port Groups on an AT-8316F/SC Switch	79
Figure 29:	Port Trunking Menu	82
Figure 30:	Port Mirroring Menu	90
Figure 31:	Point-to-Point Ports	98
Figure 32:	Edge Port	99
Figure 33:	Point-to-Point and Edge Point	99
Figure 34:	VLAN Fragmentation	100
Figure 35:	Spanning Tree Menu	101
Figure 36:	STP Menu	105
Figure 37:	STP Port Parameters Menu	107
Figure 38:	Configure STP Port Settings Menu	108

Figure 39: Display STP Port Configuration Window	109
Figure 40: RSTP Menu	110
Figure 41: RSTP Port Parameters Menu	111
Figure 42: Configure RSTP Port Settings Menu	112
Figure 43: Display RSTP Port Configuration Window	115
Figure 44: Display RSTP Port State Window	116
Figure 45: Port-based VLAN Example	123
Figure 46: Tagged VLAN Example	127
Figure 47: VLAN Menu	130
Figure 48: VLAN Definition Menu	130
Figure 49: Create VLAN Menu	131
Figure 50: Modifying VLAN Menu	134
Figure 51: Show All VLANs Window	137
Figure 52: Delete VLAN Menu	138
Figure 53: Configure Port Priorities Menu	141
Figure 54: Show Port VLANs and Priorities Window	142
Figure 55: System Config Menu	145
Figure 56: MAC Menu	149
Figure 57: Show all MAC addresses Window	150
Figure 58: Show all static MAC addresses Window	151
Figure 59: Show all multicast MAC addresses Window	152
Figure 60: Show MAC addresses on base ports Window	153
Figure 61: Configure Port Priorities Menu	163
Figure 62: Show Port VLANs & Priorities Window	165
Figure 63: IGMP Snooping Configuration Menu	169
Figure 64: View Multicast Hosts List Window	172
Figure 65: View Multicast Routers List Window	173
Figure 66: Ethernet Statistics Menu	175
Figure 67: Display Port Statistics Window	175
Figure 68: Display Module Statistics Window	177
Figure 69: Downloads & Uploads Menu	182
Figure 70: Local Management Window	186
Figure 71: Send File Window	186
Figure 72: XModem File Send Window	187
Figure 73: Entering an IP Address in the URL Field	190
Figure 74: Home Page	191
Figure 75: Exit Confirmation Window	192
Figure 76: Configuration - General Window	194
Figure 77: Monitoring - General Window	200
Figure 78: Configuration - SNMP Window	202
Figure 79: Monitoring - Ping Client Window	204
Figure 80: Configuration - Factory Default Window	205
Figure 81: Configuration - Port Settings Window	207
Figure 82: Example of Settings for Port(s) Window	208
Figure 83: Port Monitoring Page	210
Figure 84: Port Status Window	211
Figure 85: Port Statistics Window	213
Figure 86: Port Security Menu	215
Figure 87: Port Trunking Tab Window	217
Figure 88: Port Trunking Window - Create	218
Figure 89: Example of Port Trunking Window - Modify	219
Figure 90: Port Mirroring Window	223
Figure 91: Port Mirroring Window	224
Figure 92: Configuration - Spanning Tree Window	228
Figure 93: STP Configuration Spanning Tree Window	233

Figure 94: STP Settings Window	234
Figure 95: Monitoring - Spanning Tree Window	235
Figure 96: Monitoring - STP Settings Window	236
Figure 97: RSTP Configuration Spanning Tree Window	238
Figure 98: RSTP Settings Window	239
Figure 99: Monitoring - Spanning Tree Window	240
Figure 100: Monitoring - RSTP Settings Window	241
Figure 101: Configuration - VLAN Window	243
Figure 102: Add VLAN Window	243
Figure 103: View/Update VLAN Window	245
Figure 104: Monitoring - VLAN Window	248
Figure 105: View VLAN Window	248
Figure 106: COS Setting Window	250
Figure 107: Configuration - General Window	252
Figure 108: MAC Address Window	255
Figure 109: Example of MAC Address Table	256
Figure 110: Add Static MAC Address window	258
Figure 111: Configuration - General Window	260
Figure 112: COS Setting Window	263
Figure 113: Configuration - IGMP Window	266
Figure 114: Monitoring - IGMP Window	269
Figure 115: View Multicast Hosts List Window	270
Figure 116: View Multicast Routers List Window	271

List of Tables

Table 1:	Basic Switch Parameters	43
Table 2:	Port Configuration Parameters	61
Table 3:	Port Status Parameters	65
Table 4:	Trunked Ports on 10/100 Mbps and 100 Mbps Expansion Modules	81
Table 5:	Port Mirroring Parameters	90
Table 6:	Bridge Priority Value Increments	94
Table 7:	Auto-Detect Port Costs	95
Table 8:	Port Priority Value Increments	96
Table 9:	STP and RSTP Parameters	102
Table 10:	Port Assignments of the Port-based VLAN Example	124
Table 11:	Show all MAC address Parameters	150
Table 12:	Show all multicast MAC addresses Parameters	152
Table 13:	IGMP Snooping Configuration Parameters	170
Table 14:	View Multicast Hosts List Parameters	172
Table 15:	View Multicast Routers List Parameters	173
Table 16:	Port and Module Statistics Parameters	176
Table 17:	Configuration - General Window Parameters	195
Table 18:	Monitoring - General Window Parameters	201
Table 19:	Port Setting Parameters	208
Table 20:	Port Status Parameters	211
Table 21:	Port Statistics Parameters	213
Table 22:	STP and RSTP Parameters	230
Table 23:	MAC Address Parameters	255
Table 24:	MAC Address Table Parameters	256
Table 25:	COS Setting Parameters	264
Table 26:	View Multicast Hosts List Parameters	270
Table 27:	View Multicast Routers List Parameters	271

Preface

This guide contains instructions on how to configure an AT-8300 Series switch or AT-8300 Series stack using the AT-S25 management software.

The Fast Ethernet switches in the AT-8300 Series include the following:

- ❑ AT-8316F/MT
- ❑ AT-8316F/VF
- ❑ AT-8316F/SC
- ❑ AT-8324

How This Guide is Organized

This manual is divided into three sections.

Section I: Overview

This section contains just one chapter. It reviews the different ways that you could access the AT-S25 management software on a switch.

Section II: Local and Telnet Management

The chapters in this section explain how to manage an AT-8300 Series stack from a local management interface or a Telnet management interface.

A local management interface is established by connecting a terminal or PC to the RS-232 Terminal Port on the front panel of the Master switch of the stack.

A Telnet management interface is established using the Telnet application protocol. This type of management interface can be performed from any workstation on your network that has the application protocol.

Section III: Web Browser Management

The chapters in this section explain how to manage a stack using a web browser, such as Microsoft® Internet Explorer or Netscape® Navigator, from a workstation on your network.

Document Conventions

This document uses the following conventions:

Note

Notes provide additional information.



Warning

Warnings inform you that performing or omitting a specific action may result in bodily injury.



Caution

Cautions inform you that performing or omitting a specific action may result in equipment damage or loss of data.

Contacting Allied Telesyn

This section provides Allied Telesyn contact information for technical support as well as sales or corporate information.

Online Support

You can request technical support online by accessing the Allied Telesyn Knowledge Base from the following web site:

<http://kb.alliedtelesyn.com>. You can use the Knowledge Base to submit questions to our technical support staff and review answers to previously asked questions.

E-mail and Telephone Support

For Technical Support via E-mail or telephone, refer to the Support & Services section of the Allied Telesyn web site:

<http://www.alliedtelesyn.com>.

For Sales or Corporate Information

You can contact Allied Telesyn for sales or corporate information at our web site: <http://www.alliedtelesyn.com>. To find the contact information for your country, select **Contact Us**, then **Worldwide Contacts**.

Where to Find Web-based Guides

The installation and user guides for all Allied Telesyn products are available in Portable Document Format (PDF) on our web site at **<http://www.alliedtelesyn.com>**. You could view the documents on-line or download them onto a local workstation or server.

Obtaining Management Software Updates

New releases of management software for our managed products can be downloaded from the Allied Telesyn web site:
<http://www.alliedtelesyn.com>.

Upgrading AT-S25 Version 1.5.6.2 or Earlier to Version 2.0.2 or Later

This section contains the procedures for upgrading an image file to AT-S25 Version 2.0.2 or later.



Caution

The configuration file in the AT-S25 Version 1.5.6.2 or earlier version is not compatible with the AT-S25 Version 2.0.2 or later versions of code; therefore, the user needs to save the configuration settings such as the static MAC addresses, VLAN settings, port configuration settings, etc. before downloading the latest version of code. Once the latest version of code is downloaded, these settings must be reconfigured manually.

Note

You cannot perform this procedure from a Telnet or Web Browser management interface.

Note

The switch will not forward Ethernet traffic during the software download and initialization process.

Two methods that you could use to download the image file are the TFTP and XModem methods.

- ☐ **TFTP Method:** This method is used to upgrade the software to the switch modules that are part of a stacked configuration or to the entire stack at once. This method may be performed from either a local or a remote host PC.
- ☐ **XModem Method:** This method is used to upgrade the software to an individual switch module of a stack or to a stand-alone switch module. If the switch module is a member of a stack, the stacking cable(s) must be disconnected from the module before starting this procedure. This method may be performed from a local host PC only.

Note

For faster transfer, the TFTP method is preferable.

For guidelines or background information on how to upgrade the software using TFTP, refer to **TFTP Guidelines** on page 18.

TFTP Guidelines

In the legacy code of AT-S25 Version 1.5.6.2 or an earlier version and Version 1.5.6.3, the TFTP server software runs on the switch, so the user has to use the Put command of the TFTP client software on a PC to download an image file to the switch. However, AT-S25 Version 2.0.2 and after is designed to use the TFTP client software on the switch. As a result, the user must run TFTP server on the PC to download the image file to the switch when Version 2.0.2 or later is the current software. For further information on software downloads, refer to **Chapter 14: File Downloads and Uploads** on page 178.

TFTP software is available from various sources and is included in SNMP, which can be purchased through Allied Telesyn. A command line version, is included in most UNIX variants, Windows 2000, Windows NT, and Windows XP. Please consult the documentation or the manufacturer of the software for instructions on how to use the software.

Note

This is a two-step method used to upgrade the software to the switch modules that are part of a stacked configuration or to the entire stack at once. This method may be performed from either a local or a remote host PC.

Regardless of the manufacturer, all TFTP client software will need the following information:

Host - This is the IP address of the switch to which you are downloading the software.

Binary or **ANSI** - You will need to specify binary mode (-i) for the file transfer.

Put - The Put command is used to download a new software image file to the switch.

Source file - When using the Put command to download software to the stack, enter the path and filename of the file to be downloaded onto the switch. The filename must be "ATS25_V1563.IMG" or "ATS25_V202.IMG", for example, depending on the new software image that is being downloaded.

Destination file - When using the Put command to download the software from a stack, the filename must be "ats25.img". (No path should be specified for this file.)

Example:

```
tftp -i 149.35.1.1 put c:\ats25_v1563.img ats25.img
tftp -i 149.35.1.1 put c:\ats25_v202.img ats25.img
```

Using TFTP to Download the AT-S25 Version 2.0.2 Image File to the Master Switch of the Stack

In a network consisting of several AT-8316F or AT-8324 switches, you could simplify the upgrade procedure with the two-step process below:

- ❑ First, download Version 1.5.6.3 image file "*ATS25_V1563.IMG*" to the Master switch of the stack.
- ❑ Secondly, download Version 2.0.2 image file "*ATS25_V202.IMG*" to the Master switch of the stack. In turn, the Master switch will automatically download the new image file to all the Slave switches.

To download the AT-S25 Version 2.0.2 image file to the Master switch, the process is as follows:

1. Download the AT-S25 Version 1.5.6.3 image file to the Master switch via TFTP.
2. Make sure that the source image file you are downloading is for Version 1.5.6.3 "*ATS25_V1563.IMG*".

After Version 1.5.6.3 is downloaded to the Master switch; the Master switch in turn will download the image file of this version to all the Slave switches in the stack when it boots up.

When it is rebooted, verify that the current software version is "1.5.6.3", and that all the Slave switches also booted up correctly.

3. Download the source image file for Version 2.0.2 "*ATS25_V202.IMG*" to the stack via TFTP.
4. Allow the stack to reboot automatically.

Using XModem to Download the AT-S25 Version 2.0.2 Image File

This section contains the procedure for upgrading a switch module running Version 1.5.6.2 or an earlier version to Version 2.0.2 from a local management interface using the XModem protocol. (You could also load the new software using TFTP, as explain in the previous section.)

Note

This method is used to upgrade the software to an individual switch module of a stack or to a stand-alone switch module. If the switch module is a member of a stack, the stacking cable(s) must be disconnected from the module before starting this procedure. This method may be performed from a local host PC only.

Note

Hilgraeve HyperTerminal software is used in this XModem procedure.

Note

The *ATS25_V1563.IMG* file is not required when using the XModem method.

To download the AT-S25 Version 2.0.2 image file "*ATS25_V202.IMG*" using the XModem method, perform the following procedure:

1. In HyperTerminal, verify that your current port settings are set as follows:
 - Bits per second = "9600"
 - Data bits = "8"
 - Parity = "None"
 - Stop bits = "1"
 - Flow control = "None"
2. Start the AT-S25 management software. The System Booting window as shown in Figure 1 is running.

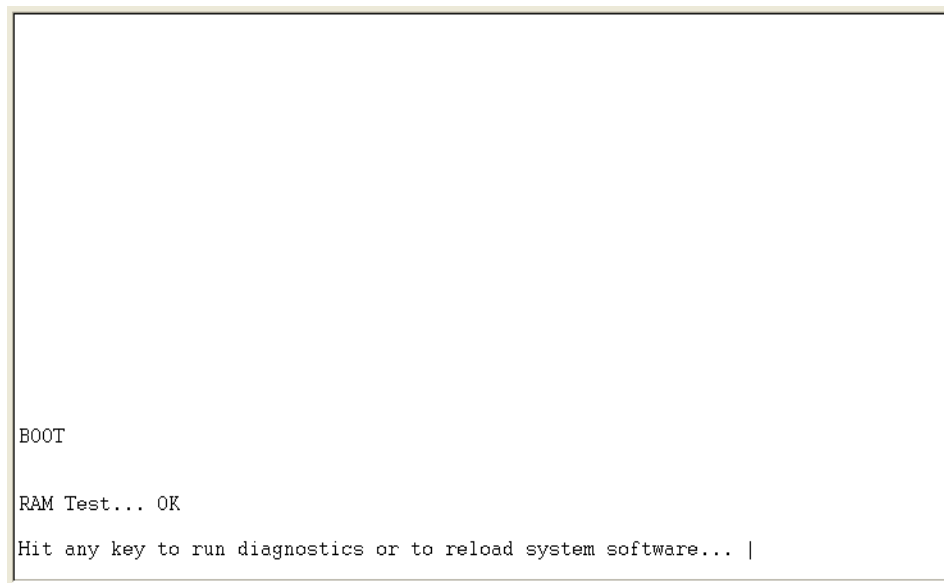


Figure 1 System Booting Window

3. Immediately hit any key to run the system diagnostics. The ATI Diagnostics menu in Figure 2 is displayed.

```

                                ATI Diagnostics
Model: AT-8324, Revision Level: 02
MAC Address: 00A0D2978F3E/00A0D2978F3E

Select an option:

R: RAM Tests
U: UART Tests
A: All of the above Tests
C: Continuous Tests
> S: Single Test

O: Other System Tests
B: BOOT System Software
X: XMODEM download updated System Software
D: Restore all configuration data to factory defaults


M: Memory Byte/Word/Dword
P: Port I/O
Z: Change Terminal Speed
-> ->


```

Figure 2 ATI Diagnostics Menu

Note

The current terminal speed is 9600 baud. For faster transfer, select the highest speed available.

4. Type **Z** to change the terminal speed.
5. Type **5** to select the new speed at 115200.
6. From the local management interface menu, select *Disconnect* from the Call menu or click the Disconnect icon  .

7. From the local management interface menu bar, select *Properties* from the File menu or click the Properties icon . The AT-S25 Properties window in Figure 3 is displayed.

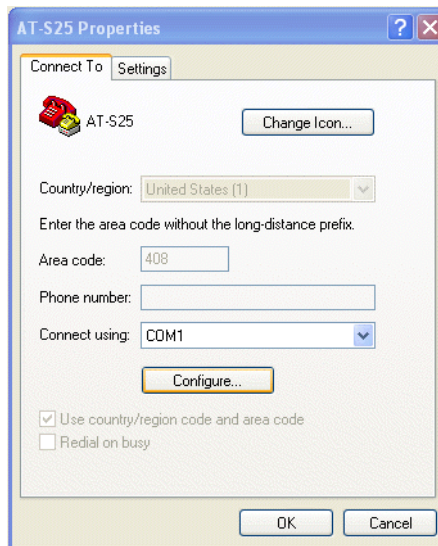


Figure 3 AT-S25 Properties Window

8. Click the Configure button. The Properties window of the connecting COM in Figure 4 is displayed.

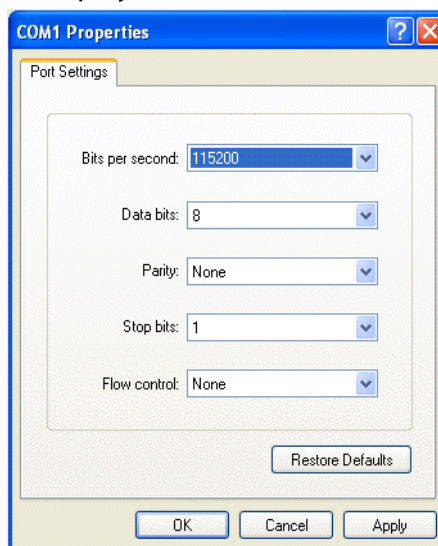




Figure 4 COM1 Properties Window

9. From the Bits per second pull-down list, select **115200**; and click **OK**. You are returned to the AT-S25 Properties.
10. In the AT-S25 Properties window, click **OK**. You are now returned to the ATI Diagnostics menu in the HyperTerminal window.

11. From the local management interface menu, select *Connect* from the Call menu or click the Call icon .
12. In the HyperTerminal window, hit any key to activate the ATI Diagnostics menu.
13. In the ATI Diagnostics menu, type **X** to select *XMODEM download updated System Software*, and press the Enter key.

The following prompt is displaying, indicating that the system is ready for the download:

```
The System is now ready for download. Please
start your XMODEM transfer.
```

14. From the HyperTerminal main window, select the Send icon  or select the Transfer menu, and then select *Send File...* from the pull-down menu, as shown in Figure 5.

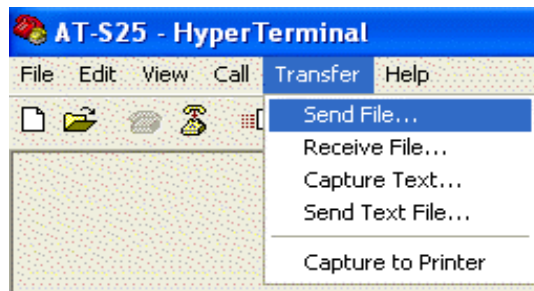


Figure 5 Local Management Window - Send File Menu

The Send File pop-up window in Figure 6 is displayed.

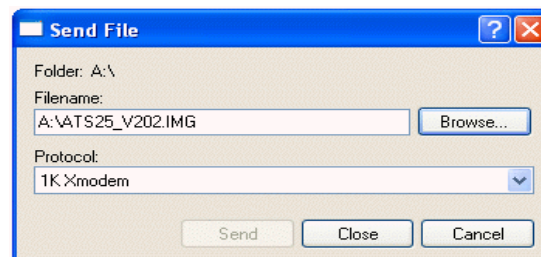


Figure 6 Send File Pop-Up Window

15. Click the Browse button to specify the location and the file to be downloaded onto the switch.
16. Click on the Protocol field and select the transfer protocol as either *Xmodem* or, for faster download, *1K XModem*.

The image file you are downloading is "ATS25_V202.IMG".

17. Click **Send**.

The software immediately begins to download onto the switch. The Xmodem File Send window in Figure 7 displays current status of the software download. The download process take a couple minutes to complete.

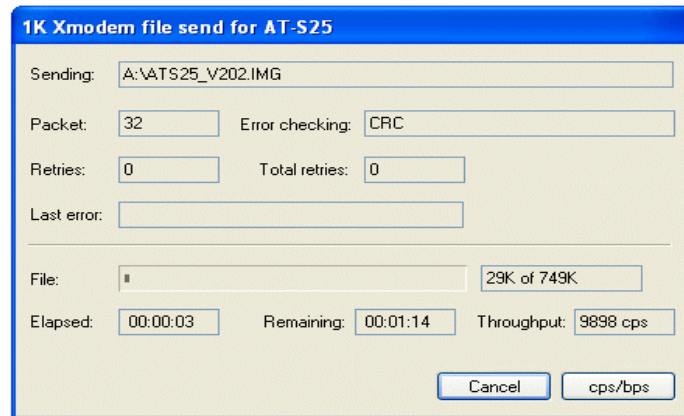


Figure 7 XModem File Send Window




Once the download process is completed, the following prompt is displayed:

```

XMODEM transfer has successfully completed.
Now writing to Flash PROM.

Please wait for FLASH writes to complete.
This may take up to 1 minute.
Do not reset, do not remove power.
The system will automatically reboot.
  
```

When the image file is downloaded to all the modules in the stack, make sure to set the terminal speed back to the default of 9600 by performing the following steps:

1. From the local management interface menu, select *Disconnect* from the Call menu or click the Disconnect icon .
2. From the local management interface menu bar, select *Properties* from the File menu or click the Properties icon . The AT-S25 Properties window in Figure 3 on page page -22 is displayed.
3. Click the Configure button. The Properties window of the connecting COM in Figure 4 on page 22 is displayed.
4. From the local management interface menu, select *Connect* from the Call menu or click the Call icon .
5. Click the Restore Defaults button, the Bits per second field is displayed with 9600 as its setting; and click **OK**.

The system is now rebooted and you are returned to the AT-S25 management software login menu.

Section I

Overview

The chapter in this section provides a brief overview of the AT-S25 management software. It explains some of the functions that you could perform with the management software and reviews the different methods for accessing the AT-S25 software on an AT-8316F or an AT-8324 Fast Ethernet Switch.

Chapter 1

Overview

The AT-S25 management software is intended for an AT-8300 Series stack of AT-8316F and AT-8324 Fast Ethernet Switches. The software is used to monitor and adjust a stack's operating parameters. Functions that you could perform with the software include:

- ☐ Enable and disable ports
- ☐ Configure port parameters, such as port speed and duplex mode
- ☐ Create virtual LANs (VLANs)
- ☐ Create port trunks and port mirrors
- ☐ Assign an Internet Protocol (IP) address and subnet mask
- ☐ Activate and configure Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP)
- ☐ Configure port security
- ☐ Configure IGMP Snooping
- ☐ Configure and View MAC Addresses
- ☐ Configure Class of Service
- ☐ File Uploads and Downloads

The AT-S25 management software comes pre-installed on the AT-8300 Series switch with default settings for all operating parameters. If the default settings are adequate for your network, you could use the switch or stack as an unmanaged Fast Ethernet switch simply by connecting the units to your network, as explained in the hardware installation guide, and powering ON the devices.

Note

The default settings for the management software can be found in **Appendix A, AT-S25 Default Settings** on page 272.

To actively manage an AT-8300 Series stack, such as to change or adjust the operating parameters, you must access the switch's AT-S25 management software. The AT-S25 software has a menu interface that makes it very easy to use.

There are four different ways that you can access the AT-S25 management software. They are briefly described in the following sections of the this chapter:

- ❑ **Local Management Session** on page 28
- ❑ **Telnet Management Session** on page 29
- ❑ **Web Browser Management Session** on page 30
- ❑ **SNMP Management Session** on page 31

Local Management Session

You establish a local management session with an AT-8300 Series stack by connecting a terminal or a PC with a terminal emulator program to the RS-232 Terminal port on the Master switch of the stack, using a straight-through RS-232 cable. This type of management interface is referred to as “local” because you must be physically close to the stack, such as in the wiring closet where the stack is located.

Once the session is started, you will see a menu from which you could make selections to configure and monitor the stack. You can configure all of the switches in a stack from a local management session.

Note

For instructions on starting a local management interface, refer to **Starting a Local Management Interface** on page 35.

Telnet Management Session

Any management workstation on your network that has the Telnet application protocol can be used to manage an AT-8300 Series stack. This type of management session is referred to in this guide as a remote management because you do not have to be in the wiring closet where the stack is located. You can manage a stack from any workstation on the network that has the application protocol.

To establish a Telnet management interface with a stack, you must assign it an IP address. Initially assigning an IP address to a stack is only possible through a local management session.

Note

For instructions on how to start a Telnet management session, refer to **Starting a Telnet Management Interface** on page 38.

A Telnet management session gives you complete access to all of a stack's operating parameters. You can perform nearly all the same functions from a Telnet management session as you can from a local management session.

Web Browser Management Session

You can also use a web browser to manage an AT-8300 Series stack. This too is referred to as remote management because you can manage a stack from any workstation on your network that has a web browser.

Note

For instructions on starting this type of management session, refer to **Starting a Web Browser Interface** on page 190.

SNMP Management Session

Another way to remotely manage a AT-8300 Series stack is with an SNMP management program. A familiarity with Management Information Base (MIB) objects is necessary for this type of management.

The AT-S25 software supports the following MIBs:

- ☐ SNMP MIB-II (RFC 1213)
- ☐ Bridge MIB (RFC 1493)
- ☐ Interface Group MIB (RFC 1573)
- ☐ Ethernet MIB (RFC 1643)
- ☐ Remote Network MIB (RFC 1757)
- ☐ Allied Telesyn Managed Switch MIB (atiStackSwitch.mib)

You must download the Allied Telesyn managed switch MIB file from the Allied Telesyn web site and compile the file with your SNMP program. For instructions, refer to your SNMP management documentation.

Note

A stack must have an IP address in order to be managed with an SNMP program. Initially assigning an IP address is only possible from a local management session.

Management Access Levels

An AT-8300 Series stack has two levels of management access. They are:

- ❑ **Manager:** When you log in as a Manager, you can view and configure all of a switch's operating parameters.

The username for Manager access is "manager" and the default password is "friend".

- ❑ **Operator:** When you log in as an Operator, you can only view the operating parameters, but you cannot change values.

The username for Operator access is "operator" and the default password is "operator".

Note

The user names and the passwords are case sensitive.

Section II

Local and Telnet Management Sessions

The chapters in this section explain how to manage an AT-8300 Series stack from a local or Telnet management session. The chapters include:

- ☐ **Chapter 2: Starting a Local or Telnet Management Session** on page 34
- ☐ **Chapter 3: Basic Switch Parameters** on page 41
- ☐ **Chapter 4: Port Parameters** on page 59
- ☐ **Chapter 5: Port Security** on page 67
- ☐ **Chapter 6: Port Trunking** on page 77
- ☐ **Chapter 7: Port Mirroring** on page 88
- ☐ **Chapter 8: STP and RSTP** on page 92
- ☐ **Chapter 9: Virtual LANs** on page 117
- ☐ **Chapter 10: MAC Address Table** on page 146
- ☐ **Chapter 11: Class of Service** on page 161
- ☐ **Chapter 12: IGMP Snooping** on page 166
- ☐ **Chapter 13: Ethernet Statistics** on page 174
- ☐ **Chapter 14: File Downloads and Uploads** on page 178

Chapter 2

Starting a Local or Telnet Management Session

This chapter contains the procedure for starting a local or Telnet management session on an AT-8300 Series stack. The sections in the chapter are:

- ❑ **Local Management Session** on page 35
- ❑ **Telnet Management Session** on page 38

Local Management Session

To start a local management session on an AT-8300 Series stack, you connect a terminal or personal computer with a terminal emulator program to the RS-232 Terminal Port on the Master switch in the stack, using a straight-through RS-232 cable. Once you have started the session, you will be able to manage all of the switches in the stack.

A local management interface is so named because you must be close to the switch, usually within a few meters, to start this type of management interface. This typically means that you must be in the wiring closet where the switch is located.

The stack does not need an IP address to be managed from a local management interface. Furthermore, running a local management session does not interfere with the flow of Ethernet traffic through the stack.

Starting a Local Management Interface

To start a local management interface, perform the following procedure:

1. Connect one end of a straight-through RS-232 cable with a DB-9 connector to the RS-232 Terminal Port on the Master switch in the stack.

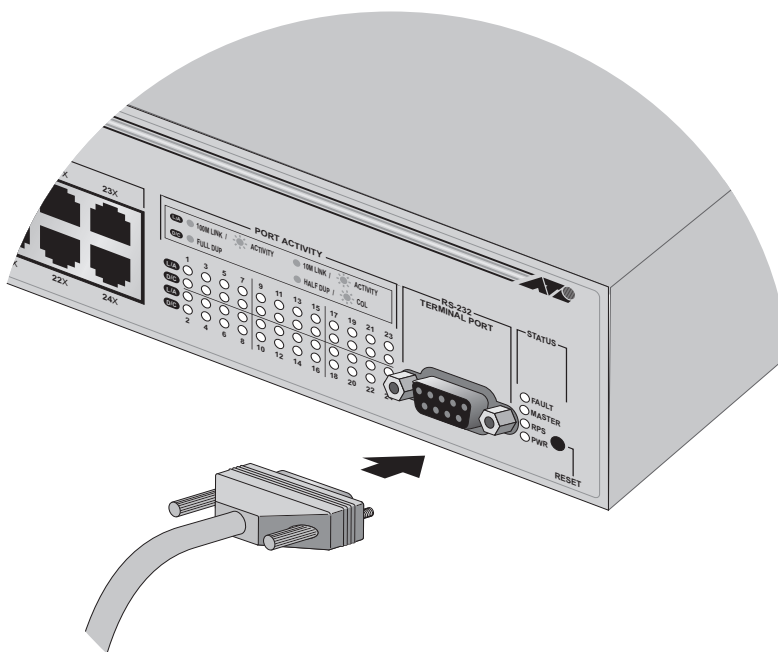


Figure 8 Connecting a Terminal or PC to the RS-232 Terminal Port

The master switch is the switch assigned the Stack ID value of 1. For information on Stack ID switch settings, refer to the *AT-8316F/MT, AT-8316F/VF, AT-8316F/SC, and AT-8324 Installation Guide*.

Note

Do not connect the terminal to the RS-232 port on a slave switch. To start a local management interface on a stack, you must connect the terminal to the RS-232 port on the master switch.

2. Connect the other end of the cable to an RS-232 port on a terminal or PC with a terminal emulator program.
3. Configure the terminal or terminal emulator program as follows:
 - ☐ Baud rate: 9600 bps
 - ☐ Data bits: 8
 - ☐ Parity: None
 - ☐ Stop bits: 1
 - ☐ Flow control: None

Note

The port settings are for a DEC VT100 or ANSI terminal, or an equivalent terminal emulator program.

When prompted for the user name and password, enter one of the following options:

4. When prompted for a user name and password, do one of the following:
 - ☐ For Manager access, type **manager** as the user name. The default password is "friend".
 - ☐ For Operator access, type **operator** as the user name. The default password is "operator".

Note

The user names and passwords are case sensitive.

The user names cannot be changed. For instructions on how to change a password, refer to **Configuring the Management Passwords** on page 51. For information on the two access levels, refer to **Management Access Levels** on page 32.

The Main Menu window is displayed in Figure 9.

```

Allied Telesyn Ethernet Switch AT-8324 - AT-S25 v2.0.2
Sales
Login Session: Manager                               Module 1 / MASTER

Main Menu

1 - Ports Menu
2 - VLAN Menu
3 - Spanning Tree Menu
4 - Administration Menu
5 - System Config Menu
6 - MAC Menu
7 - Ethernet Statistics
8 - Diagnostics Menu

S - Save Configuration changes
Q - Quit

M - Select another module

Enter your selection?

```

Figure 9 Main Menu

To select a menu item, type the corresponding letter or number.

Pressing the Esc key or typing the letter "R" in a submenu or window returns you to the previous menu.

Quitting from a Local Interface

To quit a local management interface, return to the Main Menu and type **Q** for Quit.

Note

You should always exit from a management session when you are finished managing a stack. This can prevent unauthorized individuals from making changes to a stack's configuration should you leave your management station unattended.

Note

If the console is not active for specified period of time, the console will time out.

Note

You cannot operate both a local management session and a Telnet management session on the same stack simultaneously. Failure to properly exit from a management session may block future management sessions.

Telnet Management Session

You can use the Telnet application protocol from a workstation on your network to manage an AT-8300 Series stack. This type of management is referred to as remote management because you do not have to be physically close to the switch to start the interface, as with a local management session. Any workstation on your network that has the application protocol can be used to manage the switch.

In terms of functionally, there are almost no differences between managing a switch locally through the RS-232 Terminal Port and remotely with the Telnet application protocol. You see the same menu selections and have nearly the same management capabilities.

Starting a Telnet management session requires that an IP address be assigned to the stack. Initially assigning an IP address to a stack is possible only through a local management session.

Once you have started a Telnet management interface on an AT-8300 Series stack, you have management access to all the switches that reside in the stack.

Starting a Telnet Management Interface

To start a Telnet management interface, specify the IP address of the Master switch of the stack in the Telnet application protocol.

Note

For instructions on how to configure the IP Address on the Master switch, refer to **Configuring an IP Address and Switch Name** on page 45.

When prompted for a user name and password, do one of the following:

- ☐ For Manager access, type ***manager*** as the user name. The default password is "friend".
- ☐ For Operator access, type ***operator*** as the user name. The default password is "operator".

Note

The user names and passwords are case sensitive.

The user names cannot be changed. For instructions on how to change a password, refer to **Configuring the Management Passwords** on page 51. For information on the two access levels, refer to **Management Access Levels** on page 32.

The Main Menu of a Telnet management session is identical to the Main Menu of a local management session, shown in Figure 9 on page 37. You can perform nearly all the same functions from a Telnet management session as you can from a local management session.

The menus also function the same. To make a selection, type its corresponding number or letter. To return to a previous menu, type **R** or press the Esc key.

Note

You could run only one Telnet management interface on a stack at a time. Additionally, you cannot run both a Telnet management session and a local management session on the same stack at the same time.

Quitting from a Telnet Management Interface

To end a Telnet management interface, return to the Main Menu and type **Q** for Quit.

Selecting a Switch Module in the Stack

Most of the procedures in this guide have you select the switch module in the stack on which you want to perform the procedure.

For example, to display the status of the ports on the third switch module, you would perform the following procedure:

1. From the Main Menu, type **M** to select *M - Select another module*.

The prompt message is displayed:

```
Select Module ID: [1 to 8] ->
```

2. Enter **3** for the switch module ID, and press the Enter key.

Note

The number of each switch module in the menu corresponds to the Stack ID setting on the switch. The Stack ID setting is assigned with the Stack ID switch on the back panel of the switch. For the location of the Stack ID switch and information on how to set this switch, refer to the *AT-8316F/MT, AT-8316F/VF, AT-8316F/SC and AT-8324 Installation Guide*.

Chapter 3

Basic Switch Parameters

This chapter contains a variety of information and procedures. There is a discussion on when to assign an IP address to a switch and the different ways that you could go about it. There are also procedures for resetting the switch, activating the original switch default settings, and more.

Sections in the chapter include:

- ☐ **When Does a Switch Need an IP Address?** on page 42
- ☐ **Configuring an IP Address and Switch Name** on page 45
- ☐ **Activating the BOOTP and DHCP Services** on page 46
- ☐ **Configuring SNMP Community Strings and Trap IP Addresses** on page 54
- ☐ **Pinging a Remote System** on page 49
- ☐ **Configuring the AT-S25 Software Security Features** on page 50
- ☐ **Configuring SNMP Community Strings and Trap IP Addresses** on page 54
- ☐ **Returning the AT-S25 Software to the Factory Default Values** on page 56
- ☐ **Viewing the AT-S25 Version Number and Basic Switch Information** on page 58

When Does a Switch Need an IP Address?

If you want to remotely manage an AT-8300 Series stack, you must assign it an IP address. The IP address is assigned to the Master switch of the stack and is shared by all the switches in the stack.

When you assign a stack an IP address, you must also assign it a subnet mask. The stack uses the subnet mask to determine which portion of an IP address represents the network address and which the node address.

You must also assign the stack a gateway address if there is a router between the stack and the remote management workstation. This gateway address is the IP address of the router through which the stack and management station will communicate.

If you do not intend to remotely manage an AT-8300 Series stack, then you do not need to assign it an IP address. The stack will operate fine without an IP address and you will still be able to manage it completely from a local management session.

How Do You Assign an IP Address?

Once you have decided which, if any, stacks on your network need an IP address, you have to access the AT-S25 software and assign the addresses. There are actually two ways in which an AT-8300 Series stack can obtain an IP address.

The first method is for you to assign the IP configuration information manually. The procedure for this is explained in **Configuring an IP Address and Switch Name** on page 45. Initially assigning an IP address to a switch can only be done through a local management interface.

The second method is for you to activate the BOOTP and DHCP services on the stack and have the stack automatically download its IP configuration information from a BOOTP or DHCP server on your network. This procedure is explained in **Activating the BOOTP and DHCP Services** on page 46.

The basic switch parameters can be found in the Administration Menu, as shown in Figure 10.

```

Allied Telesyn Ethernet Switch AT-8324 - AT-S25 v2.0.2
Sales
Login Session: Manager                               Module 1 / MASTER

Administration Menu

1 - IP Address ..... 0.0.0.0
2 - Subnet Mask ..... 0.0.0.0
3 - Default Gateway ... 0.0.0.0
4 - System Name ..... Sales
5 - Administrator .....
6 - Comments .....
7 - BOOTP/DHCP ..... Disabled
8 - Set Passwords

9 - Reset Switch
P - Ping a remote system
D - Downloads & Uploads Menu

S - Save Configuration changes
R - Return to Previous Menu

Enter your selection? _

```

Figure 10 Administration Menu

Table 1 lists the basic switch parameters used in the Administration Menu.

Table 1 Basic Switch Parameters

PARAMETER	DESCRIPTION
1 - IP Address	This parameter specifies the IP address of the stack. You must specify an IP address if you intend to remotely manage the stack using a Telnet utility, an SNMP management program, or a Web browser.
2 - Subnet Mask	This parameter specifies the subnet mask. You must specify a subnet mask if you assigned an IP address to the stack.
3 - Default Gateway	This parameter specifies the default router's IP address. This address is required if you intend to remotely manage the stack from a management station that is separated from the stack by a router.
4 - System Name	<p>This parameter specifies a name for the stack (for example, Sales).</p> <p>The value range is 1 to 39 alphanumeric characters. This parameter is optional.</p> <p>NOTE: Assigning names to the different stacks in your network can make it easier for you to identify them. This can help you avoid performing a configuration procedure on the wrong stack.</p>

PARAMETER	DESCRIPTION
5 - Administrator	This parameter specifies the name of the network administrator responsible for managing the stack. The value range is 1 to 39 alphanumeric characters. This parameter is optional.
6 - Comments	This parameter specifies additional information about the stack, such as its location (for example, 4th Floor - wiring closet 402B). The value range is 1 to 39 alphanumeric characters. This parameter is optional.
7 - BOOTP/DHCP	This selection activates and deactivates the BOOTP and DHCP services on the stack. For information on this selection, refer to Activating the BOOTP and DHCP Services on page 46.
8 - Set Passwords	This parameter is used to change the Manager and Operator login passwords. For instructions, refer to Configuring the Management Passwords on page 51.
9 - Reset Switch	This selection resets the stack.
P - Ping a Remote System	For information on this selection, refer to Pinging a Remote System on page 49.
D - Downloads & Uploads Menu	For information on this selection, refer to Chapter 15, File Downloads and Uploads on page 178.

Configuring an IP Address and Switch Name

The procedure in this section explains how to manually assign an IP address, subnet mask, and gateway address to an AT-8300 Series stack from a local or Telnet management interface. (If you want the stack to obtain its IP configuration from a DHCP or BOOTP server on your network, go to the procedure **Activating the BOOTP and DHCP Services** on page 46.)

This procedure also explains how to assign a name to a stack, along with other optional information, such as the name of the administrator responsible for maintaining the unit and any comments; for example, the location of the stack.

To manually assign an IP address and other information, perform the following procedure:

1. From the Main Menu, type **4** to select *Administration Menu*.

The Administration Menu as shown in Figure 10 on page 43 is displayed.

2. Make sure that the BootP/DHCP parameter is Disabled.
3. Enter or modify the parameters in the window as desired.

For information on these parameters, refer to Table 1 on page 43.

Changes to the parameters take effect immediately on the switch.

4. After you have set the parameters, type **S** to select *Save Configuration changes*.

Note

A change to a parameter in this menu, including the IP address, subnet mask, and gateway address, is immediately activated on a stack.

Activating the BOOTP and DHCP Services

The BOOTP and DHCP application protocols were developed to simplify network management. They are used to automatically assign IP configuration information to the devices on your network, such as an IP address, subnet mask, and a default gateway address.

An AT-8300 Series switch supports these protocols and can obtain its IP configuration information from a BOOTP or DHCP server on your network. If you activate this feature, a switch seeks its IP address and other IP configuration information from a BOOTP or DHCP server on your network whenever you reset or power ON the device.

Naturally, for this to work there must be a BOOTP or DHCP server residing on your network and you must configure the service by entering in the Master switch's MAC address.

BOOTP and DHCP services typically allow you to specify how the IP address is to be assigned to the switch. Choices are static and dynamic. If you choose static, the server will always assign the same IP address to the switch when the switch is reset or powered ON. This is the preferred configuration. Since the BOOTP and DHCP services always assigns the same IP address to a switch, you will always know which IP address to use when you need to remotely manage a particular switch.

If you choose dynamic, the server will assign any unused IP address that it has not already assigned to another device. This means that a switch might have a different IP address each time you reset or power cycle the device, making it difficult for you to remotely manage the unit.

Note

The BOOTP and DHCP option is disabled by default on the switch.

To activate or deactivate the BOOTP and DHCP protocols on the switch, perform the following procedure:

1. From the Main Menu, type **4** to select *Administration Menu*.

The Administration Menu in Figure 10 on page 43 is displayed.

2. Type **7** to select *BOOTP/DHCP*.

The following prompt is displayed:

```
BOOTP/DHCP (E-Enabled, D-Disabled):
```

3. Type **E** to enable BOOTP and DHCP services on the switch or **D** to disable the services and press the Enter key. The default is disabled. For information on these parameters, refer to

For information on this parameter setting, refer to Table 1 on page 43.

Note

If you activated BOOTP/DHCP, the switch immediately begins to query the network for a BOOTP or DHCP server. The switch will continue to query the network for its IP configuration until it receives a response.

Resetting a Stack

To reset a stack, perform the following procedure:

1. From the Main Menu, type **4** to select *Administration Menu*.
The Administration Menu as shown in Figure 10 on page 43 is displayed.
2. From the Administration Menu, type **9** to select *Reset Switch*.

The following prompt is displayed:

```
Do you want to proceed with the switch reboot?  
[Yes/No] ->
```

3. Type **Y** to reset the switch or **N** to cancel this procedure.

The switch reloads its operating system, a task requiring a minimum of 20 seconds to complete.

For information on this parameter setting, refer to Table 1 on page 43.



Caution

The stack will not forward traffic while it is reloading its operating software. Some data traffic may be lost.

Pinging a Remote System

You could instruct the switch to ping a remote device on your network. This procedure is useful in determining whether a valid link exists between the switch and another device.

To ping a network device, perform the following procedure:

1. From the Main Menu, type **4** to select *Administration Menu*.
The Administration Menu as shown in Figure 10 on page 43 is displayed.
2. From the Administration Menu, type **P** to select *Ping a Remote System*.

The following prompt is displayed:

```
Please enter an IP address ->
```

3. Enter the IP address of the end node you wish the switch to ping and press the Enter key.

The results of the ping command are displayed on the screen. To stop the ping, press any key.

For information on this parameter setting, refer to Table 1 on page 43.

Configuring the AT-S25 Software Security Features

The AT-S25 software has several security features that can help prevent unauthorized individuals from changing the parameter settings of an AT-8300 Series stack. The security features are:

Manager and Operator Passwords - The management software has two standard, management login accounts:

- ☐ For Manager access, type **manager** as the user name. The default password is "friend".
- ☐ For Operator access, type **operator** as the user name. The default password is "operator".

Note

The user names cannot be changed and the passwords are case sensitive. For instructions on how to change a password, refer to **Configuring the Management Passwords** on page 51. For information on the two access levels, refer to **Management Access Levels** on page 32.

Console Timeout - This parameter causes the management software to automatically end a management interface if it does not detect any activity from the local or remote management station after the specified period of time. This security feature can prevent unauthorized individuals from using your management station should you step away from your system while configuring a stack. The default for the console timeout value is 10 minutes. For instructions on how to set this security feature, refer to **Configuring Management Access** on page 52.

SNMP Access - You can also disable the SNMP management feature on a stack, and so prevent individuals from managing a stack remotely using a SNMP management program. For instructions on how to set this security feature, refer to **Configuring Management Access** on page 52.

Web Access - You can disable the web browser management feature on a stack, and so prevent individuals from managing it remotely using a web browser. For instructions on how to set this security feature, refer to **Configuring Management Access** on page 52.

Configuring the Management Passwords

There are two levels of management access on an AT-8300 Series stack: Manager and Operator. When you log in as a Manager, you can view and configure all of a stack's operating parameters. When you log in as an Operator, you can only view the operating parameters; you cannot change any values.

You log in as a Manager or an Operator by entering the appropriate password when you start an AT-S25 management software.

- ☐ The default login password for Manager access is "friend".
- ☐ The default password for Operator access is "operator".

Note

The passwords are case sensitive.

To change the Manager or Operator password, perform the following procedure:

1. From the Main Menu, type **4** to select *Administration Menu*.
The Administration Menu as shown in Figure 10 on page 43 is displayed.
2. From the Administration Menu, type **8** to select *Set Passwords*. The Passwords Menu in Figure 11 is displayed.

```

Allied Telesyn Ethernet Switch AT-8324 - AT-S25 v2.0.2
Sales
Login Session: Manager                               Module 1 / MASTER

                                Passwords Menu

1 - Set Manager Password
2 - Set Operator Password

S - Save Configuration changes
R - Return to Previous Menu

Enter your selection? _

```

Figure 11 Passwords Menu

3. Type **1** to change the Manager password, or type **2** to change the Operator password.
4. When prompted, enter the current Manager or Operator password.
5. When prompted, enter the new Manager or Operator password.

- 6. When prompted, re-enter the new Manager or Operator password.
For information on these parameters, refer to Table 1 on page 43.

Note
The password can be from 0 to 15 alphanumeric characters. The passwords are case sensitive.

Caution
You should not use spaces or special characters, such as asterisks (*) and exclamation points (!), in a password if you will be managing the stack from a web browser. Many web browsers cannot handle special characters in passwords.

**Configuring
Management
Access**

To configure the console timer, web access, SNMP access, and TFTP server security features of the AT-S25 management software, perform the following procedure:

- 1. From the Main Menu, type **5** to select *System Config Menu*.
The System Config Menu in Figure 12 is displayed.

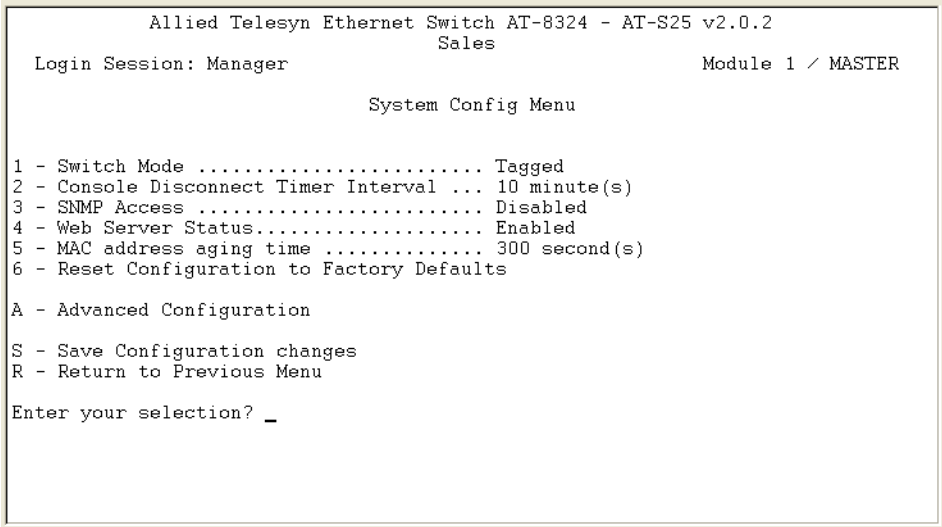


Figure 12 System Config Menu

- 2. To configure the console timer, type **2** to select *Console Disconnect Timer Interval* and, when prompted, enter a value of from 1 to 60 minutes. The default is 10 minutes.

For example, if you specify 2 minutes, the AT-S25 management software automatically ends a management interface if it does not detect any activity from the local or telnet management station after 2 minutes.

3. To configure SNMP access, type **3** to select *SNMP Access*. When prompted, type **E** to enable SNMP management access or **D** to disable it. By default, SNMP Access is Disabled.

With the SNMP Access disabled, no one will be able to manage the stack remotely using an SNMP management program.

4. To configure web browser access, type **4** to select *Web Server Access*. When prompted, type **E** to enable web access or **D** to disable web access. By default, Web Server Access is Enabled.

If the Web Server Access is disabled, no one will be able to manage the stack remotely using a web browser.

5. After you have made the desired changes, type **S** to select *Save Configuration changes*.
6. Your changes are immediately activated on the stack.

Configuring SNMP Community Strings and Trap IP Addresses

To configure the SNMP community strings for the switch and to assign up to four IP addresses of management stations to receive traps from the switch, perform the following procedure:

1. From the Main Menu, type **5** to select *System Config Menu*.

The System Config Menu as shown in Figure 12 on page 52 is displayed.

2. From the System Config Menu, type **A** to select *Advanced Configuration*.

The Advanced Configuration menu in Figure 13 is displayed.

```

Allied Telesyn Ethernet Switch AT-8324 - AT-S25 v2.0.2
Sales
Login Session: Manager                               Module 1 / MASTER

Advanced Configuration

1 - IGMP Snooping Configuration
2 - SNMP Configuration
R - Return to Previous Menu
Enter your selection? _
```

Figure 13 Advanced Configuration Menu

3. From the Advanced Configuration window, type **2** to select *SNMP Configuration*. The SNMP Configuration menu in Figure 14 is displayed.

```

Allied Telesyn Ethernet Switch AT-8324 - AT-S25 v2.0.2
Sales
Login Session: Manager                               Module 1 / MASTER

SNMP Configuration

1 - GET Community ..... public
2 - SET Community ..... private
3 - TRAP Community ..... public

4 - Trap Receiver 1 ..... 0.0.0.0
5 - Trap Receiver 2 ..... 0.0.0.0
6 - Trap Receiver 3 ..... 0.0.0.0
7 - Trap Receiver 4 ..... 0.0.0.0

S - Save Configuration changes
R - Return to Previous Menu

Enter your selection? _

```

Figure 14 SNMP Configuration Menu

4. Enter or modify the parameters as desired.

To change a value, type its corresponding number and, when prompted, enter the new value.

- ☐ To set a switch's SNMP community strings, use the parameters described below:

- 1 - GET Community
- 2 - SET Community
- 3 - TRAP Community

- ☐ To specify the IP addresses of up to four management workstations on your network to receive traps from the switch, use the selections below:

- 4 - Trap Receiver 1
- 5 - Trap Receiver 2
- 6 - Trap Receiver 3
- 7 - Trap Receiver 4

5. After making your changes, type **S** to select *Save Configuration changes*.

Changes to the SNMP parameters are immediately activated on the switch.

Returning the AT-S25 Software to the Factory Default Values

The procedure in this section returns all AT-S25 software parameters to their default values. This procedure also deletes any VLANs that you have created on the switch.

Note

The AT-S25 software default values can be found in **Appendix A, AT-S25 Default Settings** on page 272.

To return the AT-S25 management software to its default settings, perform the following procedure:

1. From the Main Menu, type **5** to select *System Config Menu*.
The System Config Menu as shown in Figure 12 on page 52 is displayed.
2. From the System Config Menu, type **6** to select *Reset Configuration to Factory Defaults*.

The following prompt is displayed:

```
The switch will reboot after set to factory default.
```

```
Do you want to proceed? [Yes/No] ->
```

3. Type **Y** for yes or **N** for no.

The following prompt is displayed:

```
Do you want to reset static IP, Subnet and Gateway  
as well? [Yes/No] ->
```

4. If you type **Y** for yes, all switch parameters including the IP address, subnet mask, and gateway address are changed to their default values. If you type **N** for no, all switch parameters excluding the IP address, subnet mask, and gateway address are changed to their default values.

The following prompt is displayed when **Y** is selected:

```
Configuration is set to factory default!
```

```
Reboot the switch..
```

The operating parameters are returned to their default values and the switch is reset.



Caution

If the switch is being managed remotely and its configuration has DHCP Enabled, this parameter will be set to Disabled after resetting the switch to Factory Defaults. This action will result in the loss of management until either the IP address is manually set or DHCP is enabled again via the serial port.

Viewing the AT-S25 Version Number and Basic Switch Information

The procedure in this section displays the following switch information:

- ☐ AT-S25 Version Number
 - ☐ Application Software Version
 - ☐ Application Software Build Date
 - ☐ MAC Address
 - ☐ Stack Info Menu
1. To display the information, type **8** to select *Diagnostics Menu* from the Main Menu.

The Diagnostics Menu window in Figure 15 is displayed.

```

Allied Telesyn Ethernet Switch AT-8324 - AT-S25 v2.0.2
Sales
Login Session: Manager                               Module 1 / MASTER

Diagnostics Menu

1 - Application Software Version ..... AT-S25 v2.0.2
2 - Application Software Build Date ... Tue Mar 25 15:20:05 2003
3 - MAC Address ..... 00:A0:D2:97:8F:3E

4 - Stack Info Menu

R - Return to Previous Menu

Enter your selection?
```

Figure 15 Diagnostics Menu

2. To view the stacking information, type **4** to select *Stack Info Menu*.
- The information in this Diagnostics Menu window and the sub-windows is for viewing purposes only.

Chapter 4

Port Parameters

The chapter contains the procedures for viewing and changing the parameter settings for the individual ports on a switch.

This chapter contains the following procedures:

- ❑ **Configuring Port Parameters** on page 60
- ❑ **Displaying Port Status** on page 64

Configuring Port Parameters

To configure the parameter settings for a port on a switch, perform the following procedure:

1. From the Main Menu, type **1** to select *Ports Menu*.
2. From the Ports Menu, type **M** if you wish to select a module other than the one currently displayed.

The prompt message is displayed:

```
Select Module ID: [1 to 8] ->
```

3. Enter the ID of the module you wish to select, and press the Enter key.
4. From the Ports Menu, type **1** to select *Port Configuration*.

The following prompt is displayed:

```
Start Port to configure [1 - 24] ->
```

5. Enter the number of the port you wish to configure and press the Enter key. To configure a range of ports, enter the first port of the range.

The following prompt is displayed:

```
End Port to configure [1 - 24] ->
```

6. To configure only one port, enter the same port number in Step 4 and Step 5, then press the Enter key. To configure a range of ports, enter the last port number in the range.

Note

Only a continuous range of ports can be entered at once.

The Port Configuration menu in Figure 16 is displayed.

```

Allied Telesyn Ethernet Switch AT-8324 - AT-S25 v2.0.2
Sales
Login Session: Manager                               Module 1 / MASTER

Port Configuration

Configuring Ports 1 to 6

1 - State ..... Enable
2 - Broadcast Filter..... Disable
3 - Negotiation ..... Auto
F - Flow Control ..... Disable
B - Back Pressure ..... Disable

S - Save Configuration changes
R - Return to Previous Menu

Enter your selection? _

```

Figure 16 Example of Port Configuration Menu

Note

The example Port Configuration window in the figure above is for a 10/100 Mbps twisted pair port. The window for a fiber optic port will contain a subset of the parameters.

7. Enter or modify the parameters in the window as desired.
Changes to the parameters take effect immediately on the switch.
- Table 2 lists the parameters used in the Port Configuration window:

Table 2 Port Configuration Parameters

PARAMETER	DESCRIPTION
1 - State	<p>Sets the current state of the selected port or the first port in the selected range.</p> <p>Settings for this parameter are:</p> <ul style="list-style-type: none"> • Enable (default): The port forwards frames. • Disable: The port will not forward frames.
2 - Broadcast Filter	<p>Sets the selected port to receive broadcast traffic.</p> <p>Settings for this parameter are:</p> <ul style="list-style-type: none"> • Enable: The port discards all ingress broadcast frames. • Disable (default): The port forwards all ingress broadcast frames.

PARAMETER	DESCRIPTION
3 - Negotiation	<p>Configures a port for Auto-Negotiation or to manually set a port's speed and duplex mode.</p> <p>Settings for this parameter are:</p> <ul style="list-style-type: none"> • Auto: Sets a port's speed and duplex mode automatically. (default) • Manual: Set a port's speed and duplex mode manually. <p>If you select <i>Auto</i>, the switch will set both speed and duplex mode for the port automatically.</p> <p>If you select <i>Manual</i>, two additional selections are displayed in the window:</p> <pre> 4 - DuplexHalf 5 - Speed 10MB </pre> <p>You use these two selections to set the port's duplex and speed mode.</p> <p>Settings for these 2 selections are:</p> <p>4 - Duplex:</p> <ul style="list-style-type: none"> • Full = Full-duplex • Half = Half-duplex <p>5 - Speed:</p> <ul style="list-style-type: none"> • 0010 = 10MB • 0100 = 100MB • 1000 = 1000MB (Optional uplink port only)
F - Flow Control	<p>Sets flow control on the port. This parameter only applies to ports operating in full-duplex mode.</p> <p>A port using flow control transmits a special pause packet to stop the end node from sending frames when the port's buffer is full and it cannot receive any more packets. The pause packet notifies the end node to stop transmitting for a specified period of time.</p> <p>Possible settings for this parameter are:</p> <ul style="list-style-type: none"> • Enable • Disable (default)

PARAMETER	DESCRIPTION
B - Back Pressure	<p>Sets back pressure on the port. This parameter only applies to ports that are operating in half-duplex mode.</p> <p>A port operating with back pressure transmits a JAM pattern to halt the transmission of packets from the end node when the port's buffer is full and it cannot receive any more packets.</p> <p>Possible settings for this parameter are:</p> <ul style="list-style-type: none">• Disable (default)• Enable

8. Once you have set the port parameters, type **S** to select *Save Configuration changes*.

Configuration changes take effect immediately on the switch.

Displaying Port Status

To display the status of the ports on the switch, perform the following procedure:

1. From the Main Menu, type **1** to select *Ports Menu*.

The Ports Menu in Figure 17 is displayed.

```

Allied Telesyn Ethernet Switch AT-8324 - AT-S25 v2.0.2
Sales
Login Session: Manager                               Module 1 / MASTER

Ports Menu

1 - Port Configuration
2 - Port Mirroring
3 - Port Trunking
4 - Port Status
5 - Port Security

A - Auto Refresh is ON

S - Save Configuration changes
M - Select another module
R - Return to Previous Menu

Enter your selection?
```

Figure 17 Ports Menu

2. From the Ports Menu window, type **M** if you want to select a module in the stack other than the one currently displayed.

The following prompt is displayed:

```
Select Module ID: [1 to 8] ->
```

3. Enter the ID of the module you want to select, and press the Enter key.
4. From the Ports Menu window, type **4** to select *Port Status*.

The Port Status window is displayed. Figure 18 is an example of the window.

```

Allied Telesyn Ethernet Switch AT-8324 - AT-S25 v2.0.2
Sales
Login Session: Manager
Module 1 / MASTER

Port Status

PortName/UplinkType State Nego Link Speed Duplex PVID FlowCtrl STP_State
-----
Port_01 Enable Auto Down ---- - 0001 -----
Port_02 Enable Auto Down ---- - 0001 -----
Port_03 Enable Auto Down ---- - 0001 -----
Port_04 Enable Auto Down ---- - 0001 -----
Port_05 Enable Auto Down ---- - 0001 -----
Port_06 Enable Auto Up 100MB Half 0001 Disable -----
Port_07 Enable Auto Down ---- - 0001 -----
Port_08 Enable Auto Down ---- - 0001 -----

N - Next Page
U - Update Display
R - Return to Previous Menu

Enter your selection? _

```

Figure 18 Port Status Window

Table 3 lists the parameters appeared in the Port Configuration window. These parameters are for viewing purposes only.

Table 3 Port Status Parameters

PARAMETER	DESCRIPTION
PortName/ UplinkType	The name of the port or, in the case of an optional uplink port, the uplink model (AT-A14, AT-A15, AT-A17, AT-A18, or AT-A19).
State	The current state of the port. Possible settings for this parameter are: <ul style="list-style-type: none"> • Enable (default) • Disable
Nego	The status of Auto-Negotiation on the port. Possible settings for this parameter are: <ul style="list-style-type: none"> • Auto - Indicates that the port is using Auto-Negotiation to set operating speed and duplex mode. • Manual - Indicates that the operating speed and duplex mode have been set manually.

PARAMETER	DESCRIPTION
Link	<p>The status of the link between the port and the end node connected to the port.</p> <p>Possible settings for this parameter are:</p> <ul style="list-style-type: none"> • Up - indicates that a valid link exists between the port and the end node. • Down - indicates that the port and the end node have not established a valid link.
Speed	<p>The operating speed of the port.</p> <p>Possible settings for this parameter are:</p> <ul style="list-style-type: none"> • 10 Mbps = 10 MB • 100 Mbps = 100 MB • 1000 Mbps = 1 GB (Optional uplink ports only)
Duplex	<p>The duplex mode of the port.</p> <p>Possible settings for this parameter are:</p> <ul style="list-style-type: none"> • Half-duplex • Full-duplex
PVID	The port VLAN identifier assigned to the port.
FlowCtrl	<p>The flow control setting for the port.</p> <p>Possible settings for this parameter are:</p> <ul style="list-style-type: none"> • Enable • Disable
STP_State	<p>The current operating STP status of the port.</p> <p>Possible settings for this parameter are:</p> <ul style="list-style-type: none"> • Disable • Blocking • Listening • Learning • Forwarding

Chapter 5

Port Security

This chapter contains the procedures for setting port security. The sections in this chapter include:

- ❑ **Port Security Overview** on page 68
- ❑ **Configuring Limited Security Level** on page 72
- ❑ **Activating a Port Security Level** on page 75

Note

You can set port security only from a local management session. You cannot set it from a Telnet management session.

Port Security Overview

The port security feature can enhance the security of your network. You can use the feature to control which network devices can forward frames through the stack.

There are four levels of port security. Only one security level can be active on an AT-8300 Series stack at a time. The security levels are:

- ☐ Automatic
- ☐ Limited
- ☐ Secure
- ☐ Lock All Ports

Note

Only one security level can be active on a stack at a time. You cannot assign different security levels on different switches in the same stack.

Automatic

This mode disables port security. Each switch in the stack learns and adds addresses to the dynamic MAC Address Table as it receives frames on the ports. MAC addresses of inactive nodes are deleted from the table according to the aging timer.

Note

The Automatic security mode is the default security level for a stack.

Limited

This security level allows you to manually specify the maximum number of dynamic MAC addresses a group of ports on a switch can learn. Once a group has learned its maximum limit, the ports within the group discard ingress frames with source MAC addresses not already stored in the MAC Address Table.

Before using this security level, please note the following:

- ☐ The maximum number of MAC addresses that a group of ports can learn applies to the entire group, not to the individual ports.
- ☐ Once this mode is activated, the switches in the stack delete all MAC addresses in the dynamic MAC Address Tables and immediately begin learning new addresses, adding them to the dynamic MAC Address Tables until a group reaches the maximum limit.

- ❑ The MAC address aging time is disabled under this security level. Once a dynamic MAC address has been learned on a port and added to a MAC Address Table, it remains in the table and is not purged unless one member of the group experiences a link down condition or the switch is power cycled.
- ❑ Static MAC addresses are retained and are not included in the count of maximum addresses that can be learned by a port group. You can continue to add static MAC addresses to a port even if the group in which the port is a member has already learned its maximum number of dynamic MAC addresses.

Port Groupings

As noted earlier, a maximum limit of MAC addresses applies to a port group. It cannot be set on a per port basis, except for some optional uplink ports. Different port groups on a switch can have different maximum limits.

Port groupings differ depending on the switch model. An AT-8324 Switch has five port groups, as illustrated in Figure 19.

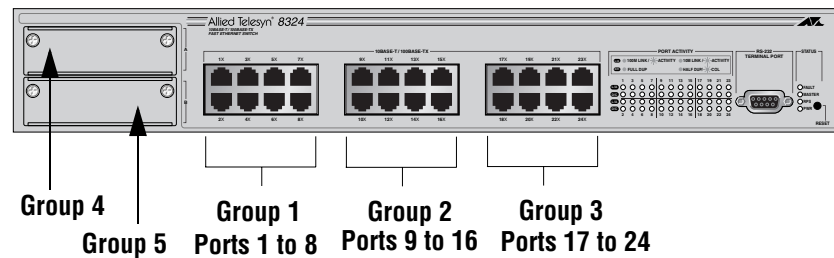


Figure 19 Port Groupings on an AT-8324 Switch

The AT-8316F/MT and AT-8316F/VF switches have four groups, as shown in Figure 20.

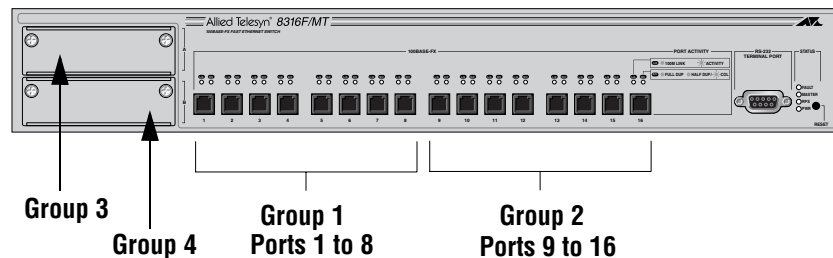


Figure 20 Port Groups on an AT-8316F/MT or AT-8316/VF Switch

The AT-8316F/SC switch also has four groups, as shown in Figure 21.

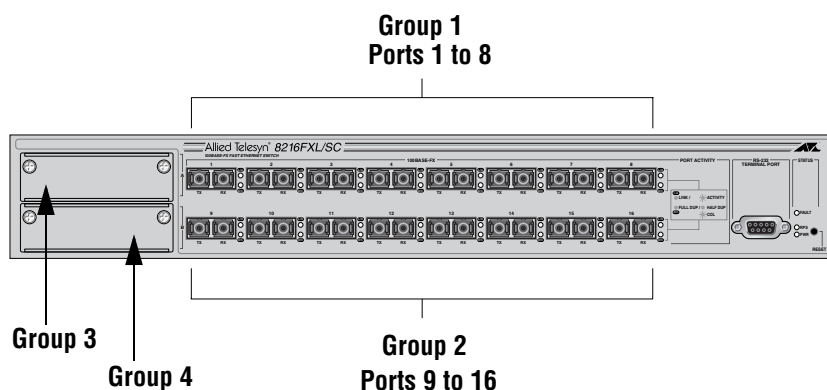


Figure 21 Port Groups on an AT-8316F/SC Switch

Here is an example of Limited port security. Let's assume you are configuring Limited port security on an AT-8324 switch and you specified that Group 1 on the switch could learn up to 50 dynamic MAC addresses. This means that Ports 1 to 8 on the switch could learn a group total of 50 dynamic MAC addresses. Once 50 dynamic addresses are learned, the ports in the group will not learn any more and will discard packets with new source addresses.

It should be noted that in some circumstances some ports in a group might not learn any MAC addresses at all. For instance, referring again to our example, if Ports 1 to 6 in Group 1 were to learn a total of 50 addresses before Ports 7 and 8 had received any packets, the latter ports would not be allowed to learn any addresses, even when they receive packets, because the group total has already been reached. This needs to be taken into account when using Limited port security.

Limited port security also applies to optional uplink ports. If the optional expansion card contains only one uplink port, then the group maximum applies to the one port. If the expansion card contains multiple uplink ports, then the maximum total of MAC addresses applies to all the ports on the card.

Secure This security level instructs the stack to forward frames based only on static MAC addresses. When this security level is activated, the stack deletes all dynamic MAC addresses and disables the MAC Address Tables in the switches in the stack so that no addresses can be learned.

The stack also deletes all static MAC addresses from the MAC Address Tables. After activating this security level, you must enter the static MAC addresses of the nodes whose frames the stack should forward. The stack will forward frames only from those nodes whose MAC addresses you enter in as static MAC addresses. Frames from nodes whose MAC addresses are not entered as static addresses will be discarded.

Lock All Ports

This security level causes the stack to stop learning new dynamic MAC addresses. The stack forwards frames based on the dynamic MAC addresses that it has already learned and any static MAC addresses that the network administrator has entered. You can add more static MAC addresses once this security level is activated.

The MAC aging time is disabled in this security level; no dynamic MAC addresses are deleted from the MAC Address Table, even those belonging to inactive end nodes.

Note

For background information on MAC addresses and aging time, refer to **MAC Address Overview** on page 147.

Configuring Limited Security Level

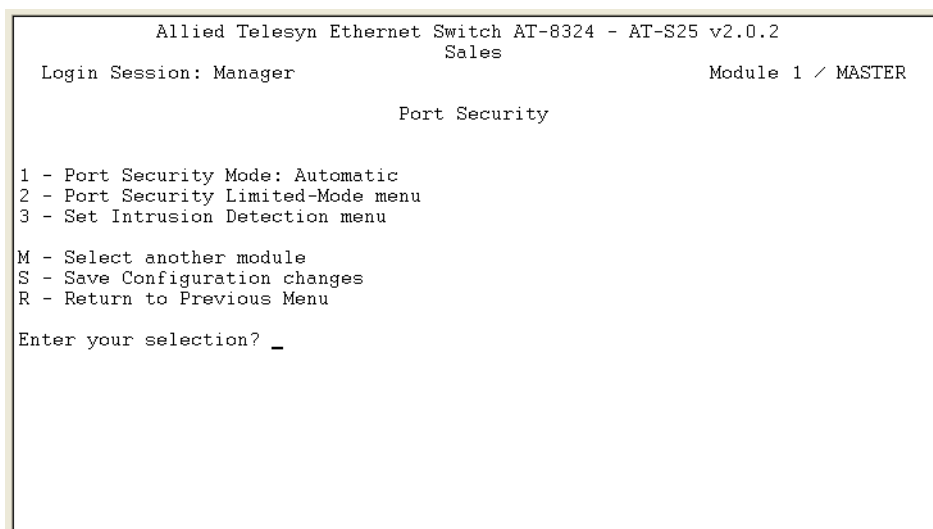
Perform the following procedure if you intend to activate the Limited security level on the stack. This procedure explains how to set the maximum number of MAC addresses the port groups can learn. (The default is 100.) You must set these values before you activate Limited security level. If you want to set the stack to the Automatic, Secured, or Lock All Ports security level, skip this procedure and go to **Activating a Port Security Level** on page 75.

Note

This procedure can only be performed from a local management session. You cannot perform it from a Telnet management session.

1. From the Main Menu, type **1** to select *Ports Menu*.
2. From the Ports Menu, type **5** to select *Port Security*.

The Port Security menu in Figure 24 is displayed.



```
Allied Telesyn Ethernet Switch AT-8324 - AT-S25 v2.0.2
Sales
Login Session: Manager                               Module 1 / MASTER

Port Security

1 - Port Security Mode: Automatic
2 - Port Security Limited-Mode menu
3 - Set Intrusion Detection menu

M - Select another module
S - Save Configuration changes
R - Return to Previous Menu

Enter your selection? _
```

Figure 22 Port Security Menu

3. From the Port Security menu, type **2** to select *Port Security Limited-Mode menu*.

The Port Security Limited-Mode menu in Figure 23 is displayed.

```

Allied Telesyn Ethernet Switch AT-8324 - AT-S25 v2.0.2
Sales
Login Session: Manager                               Module 1 / MASTER

Port Security Limited-Mode menu

1 - Display MAC Threshold
2 - Set MAC Threshold

M - Select another module
S - Save Configuration changes
R - Return to Previous Menu

Enter your selection? _

```

Figure 23 Port Security Limited-Mode Menu

4. From the Port Security Limited-Mode menu, type **M** if you want to configure the Limited security level on a switch other than the one currently managing.

The prompt message is displayed:

```
Select Module ID: [1 to 8] ->
```

5. Enter the ID of the module you want to select, and press the Enter key.
6. From the Port Security Limited-Mode menu, type **2** to select *Set MAC Threshold*.

A prompt similar to the following is displayed:

```
Select Port Group ID [1 to 5] ->
```

7. Enter the number of the port group where you want to specify a new MAC address limit. The port groupings for the AT-8300 Series switches can be found in **Port Groupings** on page 69.

The following prompt is displayed:

```
Enter the MAC threshold value -> [1 to 1024] ->
```

8. Enter the maximum number of dynamic MAC addresses you want the port group to be able to learn and press the Enter key. The range is 1 to 1024 addresses. The default is 100.
9. Repeat this procedure starting with Step 4 to specify MAC address limits on other port groups.

10. Type **1** to select *Display MAC Threshold*.

The current MAC address limits for the port groups are displayed.

11. Examine the MAC limits. Check to be sure that they are correct. If you assigned different values to different port groups, be sure that the different values apply to the correct groups. If necessary, repeat this procedure to change any MAC address limits.
12. Type **S** to select Save Configuration Changes.
13. Once you have configured the maximum limits, go to the next procedure to activate the Limited security level.

Activating a Port Security Level

The following procedure explains how to activate a port security level on a stack.

Note

Before activating the Limited security level, configure the maximum number of MAC addresses each port group can learn. For instructions, refer to **Configuring Limited Security Level** on page 72.

Note

This procedure can only be performed from a local management session. You cannot perform it from a Telnet management session.

You can perform this procedure on any switch in a stack. All switches in the stack are automatically changed to the same security level. Only one security level can be active in a stack at a time.

To activate port security on a stack, perform the following procedure:

1. From the Main Menu, type **1** to select *Ports Menu*.
2. From the Ports Menu, type **5** to select *Port Security*.

The Port Security menu in Figure 24 is displayed.

```

Allied Telesyn Ethernet Switch AT-8324 - AT-S25 v2.0.2
Sales
Login Session: Manager                               Module 1 / MASTER

Port Security

1 - Port Security Mode: Automatic
2 - Port Security Limited-Mode menu
3 - Set Intrusion Detection menu

M - Select another module
S - Save Configuration changes
R - Return to Previous Menu

Enter your selection? _

```

Figure 24 Port Security Menu

3. From the Port Security menu, type **1** to select *Port Security Mode: Automatic*.

The following prompt is displayed:

```
Enter new mode (A-Automatic, L-Limited, S-Secured,  
K-lockEd) :
```

4. Select the desired security level by typing the appropriate letter. For a description of the security levels, refer to **Port Security Overview** on page 68.

A change to the security level is immediately activated on a stack.

5. Type **S** to select *Save Configuration Changes*.

Chapter 6

Port Trunking

This chapter contains the procedures for creating and deleting port trunks. Sections in the chapter include:

- ☐ **Port Trunking Overview** on page 78
- ☐ **Creating a Port Trunk** on page 82
- ☐ **Modifying a Port Trunk** on page 85
- ☐ **Modifying a Trunk Name** on page 86
- ☐ **Deleting a Port Trunk** on page 87

Port Trunking Overview

Port trunking is an economical way for you to increase the bandwidth between two switches. A port trunk is a group of 2 to 8 ports that have been grouped together to function as one logical path. A port trunk increases the bandwidth between switches and is useful in situations where a single physical data link between switches is insufficient to handle the traffic load.

A port trunk always sends packets from a particular source to a particular destination over the same link within the trunk. A single link is designated for flooding broadcasts and packets of unknown destination.

The example in Figure 25 consists of a port trunk of four data links between two AT-8324 Switches.

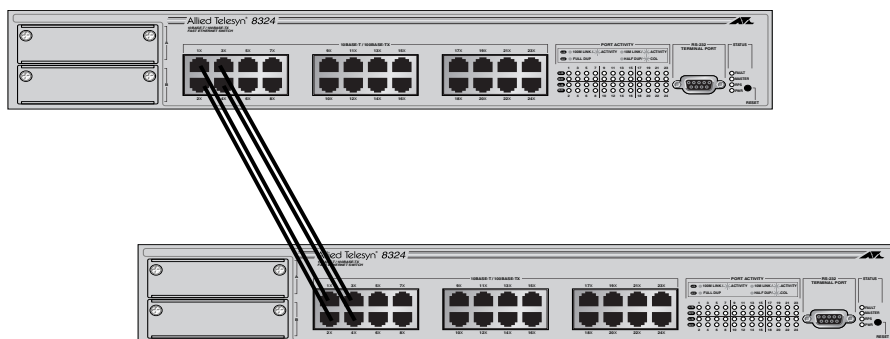


Figure 25 Port Trunk Example

Port Trunking Guidelines

When creating a port trunk, observe the following guidelines:

Selecting the Number of Ports in a Trunk

A port trunk can consist of 2 to 8 ports. .

Selecting Ports from the Same Switch in a Stack

The ports of a port trunk must be from the same switch in a stack. A port trunk cannot consist of ports from different switches in a stack.

Using Ports from the Same Group

The ports on the AT-8300 Series switch are divided into groups. When selecting ports for a trunk, the selected ports must be members of the same group.

The AT-8324 Switch has five groups, as illustrated in Figure 26.

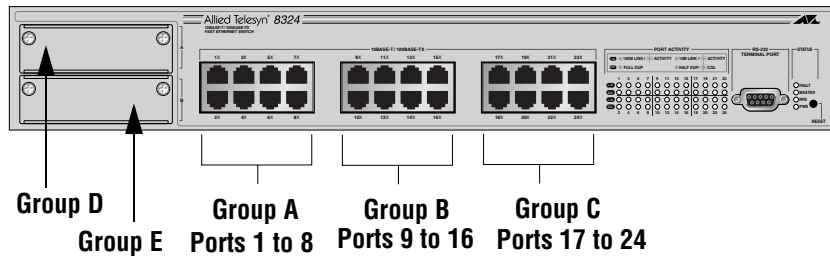


Figure 26 Port Groupings on an AT-8324 Switch

The AT-8316F/MT and AT-8316F/VF switches have four groups, as shown in Figure 27.

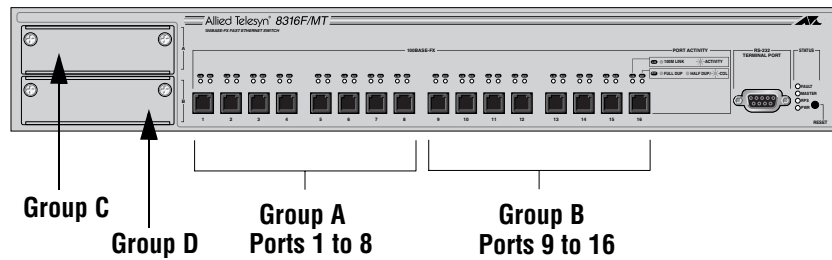


Figure 27 Port Groups on an AT-8316F/MT or AT-8316F/VF Switch

The AT-8316F/SC switch also has four groups, as shown in Figure 28.

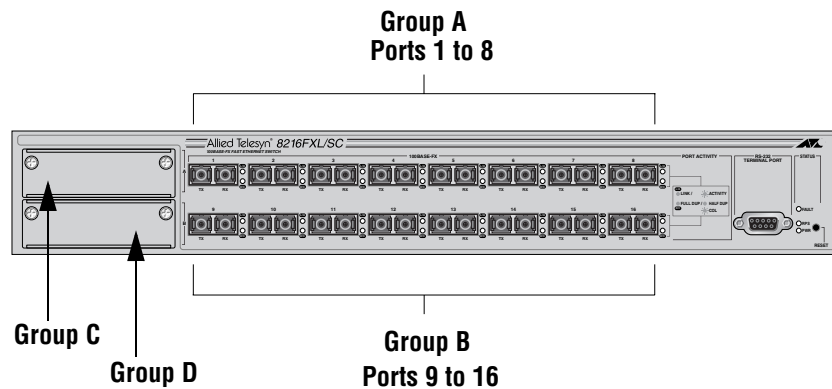


Figure 28 Port Groups on an AT-8316F/SC Switch

As an example of a port trunk on an AT-8324 Switch, you could use Ports 4 and 5 as one port trunk, since the ports are members of the same group. However, you could not use Ports 7, 8, 9, and 10 because they belong to different groups.

Creating Only One Trunk Per Group

Each port group can support one port trunk. For example, the AT-8324 Ethernet switch, which has three port groups, assuming no expansion modules, can support three port trunks, one port trunk for each port group. The addition of two expansion modules would enable the switch to support two more port trunks, one for each module.

Cabling Based on Port Number

When cabling a trunk, the order of the connections must be the same on both nodes. The lowest numbered port in a trunk must be connected to the lowest numbered port of the trunk on the other device, the next lowest numbered port must be connected to the next lowest numbered port on the other device, and so on.

For example, assume that you are connecting a trunk between two AT-8324 Switches. On the first AT-8324 Switch you had chosen Ports 12, 13, 14, 15 from port group 2 for the trunk. On the second AT-8324 Switch you had chosen Ports 21, 22, 23, and 24 from port group 3. To maintain the order of the port connections, you connect Port 12 on the first AT-8324 Switch to Port 21 on the second AT-8324, Port 13 to Port 22, and so on.

Configuring the Port Parameters of a Port Trunk

The ports of a trunk automatically assume the speed and duplex mode of the lowest numbered port in the trunk. For example, if you create a trunk consisting of Ports 4, 5, 6, and 7, Port 4's configuration is automatically propagated to Ports 5, 6, and 7. You cannot configure the ports of a trunk individually. They can be configured only as a unit.

Configuring VLANs

All ports in a trunk must belong to the same VLAN.

Creating Port Trunks on 10/100 Mbps and 100 Mbps Expansion Modules

The ports on an expansion card that contains two or more 10/100 Mbps or 100 Mbps twisted pair or fiber optic ports can be grouped together to form a port trunk, as shown in Table 4.

Table 4 Trunked Ports on 10/100 Mbps and 100 Mbps Expansion Modules

Number of Ports on Expansion Module	Port Trunks
1	Does not support port trunking.
2	One port trunk consisting of two ports.
4	One trunk consisting of two, three or four ports.

Creating Port Trunks on One Gigabit Expansion Modules

If a switch contains two expansion modules and each module has one gigabit port, you can group the two ports into one trunk. This is the only instance where you can create a port trunk from different port groups on a switch. Both gigabit modules must be installed in the same switch and both modules must be of the same medium type (i.e., either both fiber or both twisted pair).

Creating a Port Trunk

This section contains the procedure for creating a port trunk on the switch. Be sure to review the guidelines in **Port Trunking Overview** on page 78 before performing the procedure.

⚠

Caution

Do not connect the cables to the ports in a port trunk until after you have configured the trunk with the management software. Connecting the cables before configuring the software will create a loop in your network topology, possibly resulting in broadcast storms and poor network performance.

Creating a 10/100 Port Trunk

To create a 10/100 port trunk, perform the following procedure:

- From the Main Menu, type **1** to select *Ports Menu*.
- From the Ports Menu, type **3** to select *Port Trunking*.

The Port Trunking menu in Figure 29 is displayed.

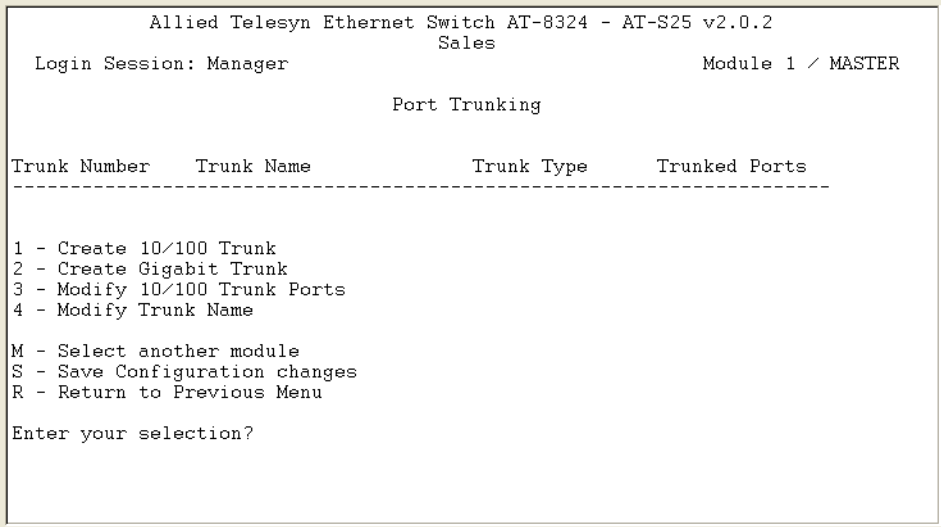


Figure 29 Port Trunking Menu

- To create the port trunk on a switch in the stack other than the one you are currently managing, type **M**.
The prompt message is displayed:

Select Module ID: [1 to 8] ->
- Enter the ID of the module you wish to select, and press the Enter key.

- From the Port Trunking menu, type **1** to select *Create 10/100 Trunk*.

The prompt similar to the following is displayed.

```
Enter Trunk Number -> [1 to 5] ->
```

- Enter the port group containing the ports to be in the trunk and press the Enter key. (For port groupings, refer to **Using Ports from the Same Group** on page 79.)

The following prompt appears:

```
Enter Trunk Name ->
```

- Enter a name for the trunk and press the Enter key. The name can be up to 10 alphanumeric characters.

A prompt similar to the following appears:

```
Enter trunk ports [1 - 8] ->
```

- Specify the ports of the trunk. You can specify the ports individually (e.g., 1,2,3,4), as a range (e.g., 1-4), or both (e.g., 1-2,5,7).

- Type **S** to select *Save Configuration Changes*.

- Configure the ports on the remote switch for port trunking.

- Connect the cables to the ports of the trunk on the switch.

The port trunk is ready for network operation.

Creating a Gigabit Port Trunk

To create a Gigabit port trunk, perform the following procedure:

- From the Main Menu, type **1** to select *Ports Menu*.

- From the Ports Menu, type **3** to select *Port Trunking*.

The Port Trunking menu in Figure 29 on page 82 is displayed.

- To create the port trunk on a switch in the stack other than the one you are currently managing, type **M**.

The prompt message is displayed:

```
Select Module ID: [1 to 8] ->
```

- Enter the ID of the module you want to select, and press the Enter key.

- From the Port Trunking menu, type **2** to select *Create Gigabit Trunk*.

The following prompt is displayed.

```
Enter Trunk Name ->
```

- Enter a name for the trunk and press the Enter key. The name can be up to 10 alphanumeric characters.

7. Type **S** to select *Save Configuration Changes*.
8. Configure the ports on the remote switch for port trunking.
9. Connect the cables to the ports of the trunk on the switch.

The port trunk is ready for network operation.

A prompt similar to the following appears:

```
Enter trunk ports [1 - 8] ->
```

```
Enter Trunk Number -> [1 to 2] ->
```

10. Enter the ports that will constitute the port trunk; then press the Enter key.

You can specify the ports individually (e.g., 24,25) or as a range (e.g., 24-25).

Once you have specified the port(s) of the trunk, the following menu selection appears in the window:

```
Enter trunk ports [1 - 8] ->
```

Press any key to continue.

Modifying a Port Trunk

To add or remove ports from a 10/100 Mbps port trunk, perform the following procedure:

1. From the Main Menu, type **1** to select *Ports Menu*.
2. From the Ports Menu, type **3** to select *Port Trunking*.

The Port Trunking menu in Figure 29 on page 82 is displayed.

3. To modify a port trunk on a switch other than the one currently selected, type **M**.

The following prompt is displayed:

```
Select Module ID: [1 to 8] ->
```

4. Enter the ID of the module you want to select, and press the Enter key.
5. From the Port Trunking menu, type **3** to select *Modify 10/100 Trunk Ports*.

The following prompt is displayed.

```
Enter Trunk Number -> [1 to 5] ->
```

6. Enter the number of the port trunk you want to modify; then press the Enter key.

The following prompt is displayed:

```
Enter trunk ports [1 - 8] ->
```

7. Enter the new port list for the trunk port. The new ports will overwrite the old ports. You can specify the ports individually (e.g., 1,2,3,4), as a range (e.g., 1-4), or both (e.g., 1-2,5,7).
8. Press any key to continue.
9. Type **S** to select *Save Configuration Changes*.

Modifying a Trunk Name

To modify the name of a port trunk, perform the following procedure:

1. From the Main Menu, type **1** to select *Ports Menu*.
2. From the Ports Menu, type **3** to select *Port Trunking*.

The Port Trunking menu in Figure 29 on page 82 is displayed.

3. To modify a port trunk on a module other than the one currently selected, type **M**.

The following prompt is displayed:

```
Select Module ID: [1 to 8] ->
```

4. Enter the ID of the module you want to select, and press the Enter key.
5. From the Port Trunking menu, type **4** to select *Modify Trunk Name*.

The following prompt is displayed.

```
Enter Trunk Number -> [1 to 6] ->
```

6. Enter the number of the port trunk you want to modify and press the Enter key.

The following prompt is displayed.

```
Enter Trunk Name ->
```

7. Enter the new name for the port trunk. The name can be up to 30 alphanumeric characters.
8. Type **S** to select *Save Configuration Changes*.

Deleting a Port Trunk



Caution

Disconnect the cables from the port trunk on the switch before performing the following procedure. Deleting a port trunk without first disconnecting the cables can create loops in your network topology, which can result in broadcast storms and poor network performance.

To delete a port trunk from the switch, perform the following procedure:

1. From the Main Menu, type **1** to select *Ports Menu*.
2. From the Ports Menu, type **3** to select *Port Trunking*.
The Port Trunking menu in Figure 29 on page 82 is displayed.
3. To delete a port trunk from a module other than the one currently selected, type **M**.
The prompt message is displayed:

```
Select Module ID: [1 to 8] ->
```
4. Enter the ID of the module you want to select, and press the Enter key.
5. From the Port Trunking menu, type **5** to select *Delete trunk*.
The following prompt is displayed:

```
Enter Trunk Number -> [1 to 6] ->
```
6. Enter the number of the trunk you want to delete.
The following prompt is displayed:

```
Are you sure you want to delete the trunk (Y/N) ->
```
7. Type **Y** for Yes to delete the port trunk or **N** for No to cancel this procedure.
If **Y** is selected, the port trunk is deleted from the switch.
8. Type **S** to select *Save Configuration changes*.

Chapter 7

Port Mirroring

This chapter contains the procedures on how to create a port mirror.
Sections in the chapter include:

- ❑ **Port Mirroring Overview** on page 89
- ❑ **Creating a Port Mirror** on page 90

Port Mirroring Overview

The port mirroring feature allows you to unobtrusively monitor the traffic being received and transmitted on a port on a switch by having the traffic copied to another switch port. You could connect a network analyzer to the port where the traffic is being copied and monitor the traffic on the other ports without impacting network performance or speed.

Observe the following guidelines when creating a port mirror:

- ☐ The port whose traffic is to be copied is called the source port. The port where the traffic is to be copied and where the network analyzer will be located is called the destination port.
- ☐ You can mirror only one port in a stack at a time.
- ☐ There can be only one destination port.
- ☐ The destination port cannot be a member of a port trunk.
- ☐ The source port and the destination port can be located on different switches in a stack.
- ☐ The source port and the destination port must be operating at the same speed. For example, you cannot use a 10/100 Mbps port to monitor traffic on a 1000 Mbps GBIC port.
- ☐ The source port and the destination port must be in the same VLAN in order to see broadcast, multicast, and flooded traffic on the destination mirror port. If these packets are being sent and received on a tagged port, they will have the tag removed before delivery to the destination mirror port.
- ☐ Unicast packets that are received on a tagged port will have the tag removed before delivery to the destination mirror port. Unicast packets sent out a tagged port will have the tag inserted before delivery to the destination port.

Creating a Port Mirror

To create a port mirror, perform the following procedure:

- 1. From the Main Menu, type **1** to select *Ports Menu*.
- 2. From the Ports Menu, type **2** to select *Port Mirroring*.

The Port Mirroring menu in Figure 30 is displayed.

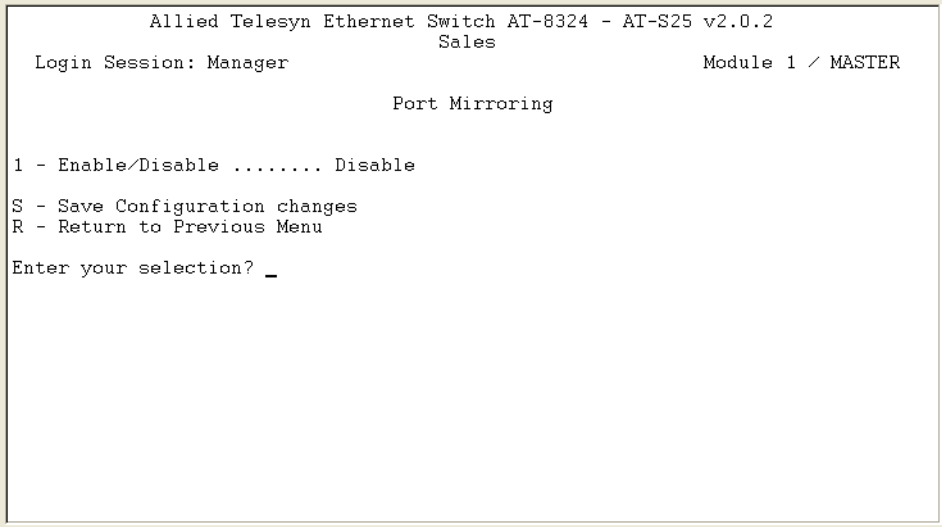


Figure 30 Port Mirroring Menu

- 3. Type **1** to select *Enable/Disable*.

The following prompt is displayed.

Enter Enable (E)/Disable (D) :

- 4. Type **E** to enable the port mirroring feature or **D** to disable the port mirroring feature. The default is disabled. Press the Enter key.
- 5. If the port mirroring is enabled, several new options are added to the Port Mirroring menu.

Table 5 lists the parameters used in the Port Mirroring Menu.

Table 5 Port Mirroring Parameters

PARAMETER	DESCRIPTION
2 - Destination Module	Use this option to specify the switch in the stack where the destination port is located.
3 - Destination Port	Use this selection to specify the destination port on the switch. This is the port where the traffic from the source port will be copied to.

PARAMETER	DESCRIPTION
4 - Source Module	Use this option to specify the switch in the stack containing the source port.
5 - Source Port	Use this option to specify the source port. This is the port whose traffic will be copied to the destination port. You can specify only one port.

6. Configure the options in the menu as needed. Refer to the table above for option definitions.
7. Type **S** to select *Save Configuration changes*.

The port mirror is immediately activated on the switch. You can now connect a data analyzer to the destination port to monitor the traffic on the source port.

Chapter 8

STP and RSTP

This chapter provides background information on the Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP). The chapter also contains procedures on how to adjust the STP and RSTP bridge and port parameters. The sections in this chapter include:

- ❑ **STP and RSTP Overview** on page 93
- ❑ **Enabling or Disabling STP or RSTP** on page 101
- ❑ **Configuring STP** on page 105
- ❑ **Displaying Port's STP Status and Setting** on page 109
- ❑ **Configuring RSTP** on page 110
- ❑ **Displaying Port's RSTP Status and Settings** on page 114

Note

For detailed information on the Spanning Tree Protocol, refer to IEEE Std 802.1d. For detailed information on the Rapid Spanning Tree Protocol, refer to IEEE Std 802.1w.

STP and RSTP Overview

A significant danger to Ethernet network performance is the existence of a data loop in a network topology. A data loop exists when two or more nodes on a network can transmit data to each other over more than one data link. The problem that data loops pose is that data packets can become caught in repeating cycles, referred to as broadcast storms, that needlessly consume network bandwidth and significantly reduce network performance.

STP and RSTP prevent data loops from forming by ensuring that only one path exists between the end nodes in your network. Where multiple paths exist, these protocols place the extra paths in a standby or blocking mode, leaving only one main active path.

STP and RSTP can also activate a redundant path if the main path goes down. So not only do these protocols guard against multiple links between segments and the risk of broadcast storms, but they can also maintain network connectivity by activating a backup redundant path in case a main link fails.

Where the two protocols differ is in the time each takes to complete the process commonly referred to as *convergence*. When a change is made to the network topology, such as the addition of a new bridge, a spanning tree protocol must determine whether there are redundant paths that must be blocked to prevent data loops, or activated to maintain intercommunications between the various network segments. This process is referred to as convergence.

With STP, convergence can take a minute or more to complete in a large network. This can result in lost data packets from the loss of intercommunication between various parts of the network during the convergence process.

RSTP is much faster. RSTP can complete a convergence in seconds, and so greatly diminish the impact the process can have on your network.

Note

RSTP is the default Active Protocol version. The Spanning Tree feature is disabled by default.

Both STP and RSTP are using the same database; therefore, they are using the same parameters. Any changes made to the common parameters will be take effect on both protocols such as: Bridge Priority, Bridge Hello Time,..."

The following subsections provide a basic overview on how STP and RSTP operate and describe the available parameters.

Bridge Priority and the Root Bridge

The first task that bridges perform when a spanning tree protocol is activated on a network is the selection of a *root bridge*. A root bridge distributes network topology information to the other network bridges and is used by the other bridges to determine if there are redundant paths in the network.

A root bridge is selected by a combination of a *bridge priority* number, also referred to as the bridge identifier, and sometimes the bridge's MAC address. The bridge with the lowest bridge priority number in the network is selected as the root bridge. If two or more bridges have the same bridge priority number, of those bridges the one with the lowest MAC address is designated as the root bridge.

The bridge priority number can be changed on an AT-8316F or an AT-8324 Switch. You could designate which switch on your network you wish as the root bridge by giving it the lowest bridge priority number. You might also consider which bridge should function as the backup root bridge in the event you need to take the primary root bridge off-line, and assign that bridge the second lowest bridge identifier number.

Bridge priority has a range of 0 to 61440 in multiples of 4096. The management software divides the range into increments. You specify the increment that represents the desired bridge priority value. The range is divided into sixteen increments, as shown in the following table.

Table 6 Bridge Priority Value Increments

Increment	Bridge Priority	Increment	Bridge Priority
0	0	8	32768
1	4096	9	36864
2	8192	10	40960
3	12288	11	45056
4	16384	12	49152
5	20480	13	53248
6	24576	14	57344
7	28672	15	61440

Path Costs and Port Costs

Once the Root Bridge has been selected, the bridges must determine if the network contains redundant paths and, if one is found, they must select a preferred path while placing the redundant paths in a backup or blocking state.

Where there is only one path between a bridge and the root bridge, the bridge is referred to as the *designated bridge* and the port through which the bridge is communicating with the root bridge is referred to as the *root port*.

If redundant paths exist, the bridges that are a part of the paths must determine which path will be the primary, active path, and which path(s) will be placed in the standby, blocking mode. This is accomplished by an determination of *path costs*. The path offering the lowest cost to the root bridge becomes the primary path and all other redundant paths are placed into blocking state.

Path cost is determined through an evaluation of *port costs*. Every port on a bridge participating in STP has a cost associated with it. The cost of a port on a bridge is typically based on port speed. The faster the port, the lower the port cost. The exception to this is the ports on the root bridge, where all ports have a port cost of 0.

Path cost is simply the cumulation of the port costs between a bridge and the root bridge.

The port costs of the ports on an AT-8316F or an AT-8324 Switch are adjustable through the management software. For either STP or RSTP, the port costs have a range of from 0 to 20 000 000. This range allows you to have more control over path costs.

These port costs also feature an Auto-Detect feature. This features allows either STP or RSTP to automatically set the port cost according to the speed of the port, assigning a lower value for higher speeds. Auto-Detect is the default setting on the ports when the switch is operating in either STP or RSTP. Table 7 lists the ports cost with Auto-Detect.

Table 7 Auto-Detect Port Costs

Port Speed	Port Cost
10 Mbps	2 000 000
100 Mbps	200 000
1000 Mbps	20 000

You could override Auto-Detect and set the port cost manually.

Port Priority

If two paths have the same port cost, the bridges must select a preferred path. In some instances this can involve the use of the *port priority* parameter. This parameter can be used as a tie-breaker when two paths have the same cost.

The port priority has a range of from 0 to 240. As with the bridge priority, this range is broken into increments, in this case multiples of 16. When you specify a port priority for a port, you enter the increment of the desired value.

Table 8 Port Priority Value Increments

Increment	Bridge Priority	Increment	Bridge Priority
0	0	8	128
1	16	9	144
2	32	10	160
3	48	11	176
4	64	12	192
5	80	13	208
6	96	14	224
7	112	15	240

Forwarding Delay and Topology Changes

If there is a change in the network topology due to a failure, removal, or addition of any active components, the active topology also changes. This may trigger a change in the state of some blocked ports. However, a change in a port state is not activated immediately.

It might take time for the root bridge to notify all bridges that a topology change has occurred, especially if it is a large network. If a topology change is made before all bridges have been notified, a temporary data loop could occur, and that could adversely impact network performance.

To forestall the formation of temporarily data loops during topology changes, a port designated to change from blocking to forwarding passes through two additional states, listening and learning, before it begins to forward frames. The amount of time a port spends in these states is set by the *forwarding delay* value. This value states the amount of time that a port spends in the listening and learning states prior to changing to the forwarding state.

During a reconvergence and for a short period of time thereafter, the switch's FDB aging time is shortened considerably. This is done to minimize the impact of possible path changes to host machines due to the topology change. The side effect of this is an increase in flooding, and may result in a small amount of packet loss.

The forwarding delay value is adjustable on the AT-8316F or AT-8324 Switch through the management software. The appropriate value for this parameter will depend on a number of variables, with the size of your network being a primary factor. For large networks, you should specify a value large enough to allow the root bridge sufficient time to propagate a topology change throughout the entire network. For small networks, you should not specify a value so large that a topology change is unnecessarily delayed, which could result in the delay or loss of some data packets.

Hello Time and Bridge Packet Data Units (BPDU)

The bridges that are part of a spanning tree domain communicate with each other using a bridge broadcast frame that contains a special section devoted to carrying STP or RSTP information. This portion of the frame is referred to as the Bridge Packet Data Unit (BPDU). When a bridge is brought on-line, it will issue a BPDU in order to determine whether a root bridge has already been selected on the network. and if not, whether it has the lowest bridge priority number of all the bridges and should therefore become the root bridge.

The root bridge will periodically transmit a BPDU to determine whether there have been any changes to the network topology and to inform other bridges of topology changes. The frequency with which the root bridge sends out a BPDU is called the *Hello Time*. This is a value that you could set on the AT-8316F or AT-8324 Switch. The interval is measured in seconds and the default is 2 seconds. Consequently, if an AT-8316F or an AT-8324 Switch is selected as the Root Bridge of a spanning tree domain, it will transmit a BPDU every two seconds.

Point-to-Point Ports and Edge Ports

Note

This section applies only to RSTP.

Part of the task of configuring RSTP is defining the port types on the bridge. This relates to the device(s) connected to the port. With port type defined, RSTP can reconfigure a network much quicker than STP when a change in network topology is detected.

There are two possible selections: Point-to-Point and Edge Port.

If a bridge port is operating in full-duplex mode, than the port is functioning as point-to-point. Figure 31 illustrates two AT-8324 Switches that have been interconnected with one data link. With the link operating in full-duplex, the ports are said to be point-to-point ports.

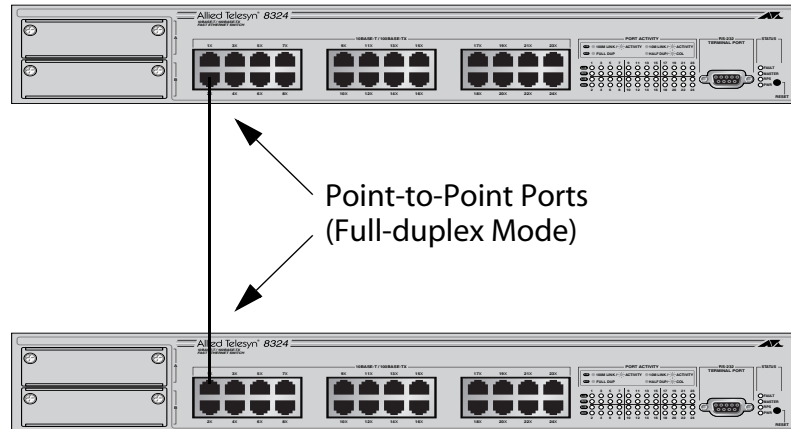


Figure 31 Point-to-Point Ports

If a port is operating in half-duplex mode and is not connected to any further bridges participating in STP or RSTP, then the port is an edge port. Figure 32 illustrates an edge port on an AT-8324 Switch. The port is connected to an Ethernet hub, which in turn is connected to a series of Ethernet workstations. This is an edge port because it is connected to a device operating at half-duplex mode and there are no participating STP or RSTP devices connected to it.

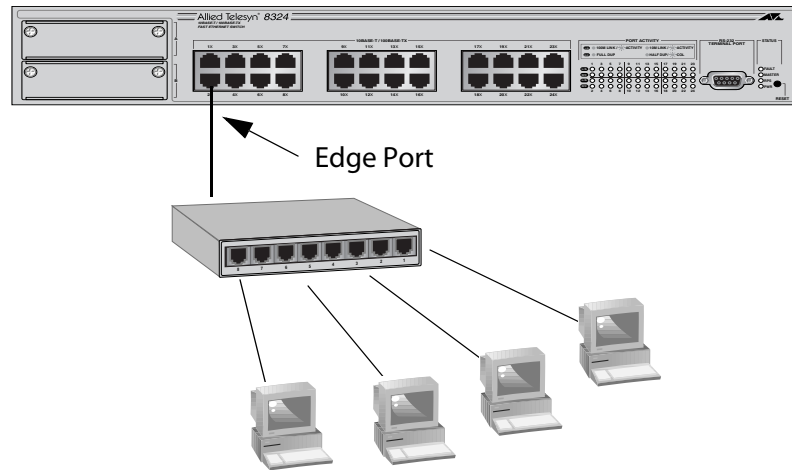


Figure 32 Edge Port

A port can be both point-to-point and edge at the same time. It would operate in full-duplex and have no STP or RSTP devices connected to it. Figure 33 illustrates a port functioning both as point-to-point and edge.

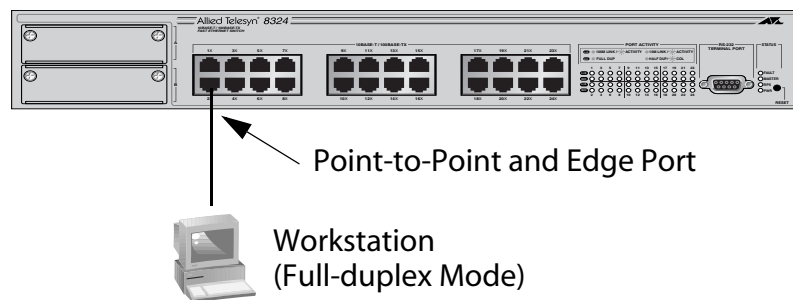


Figure 33 Point-to-Point and Edge Point

Determining whether a bridge port is point-to-point, edge, or both, can be a bit confusing. For that reason it might be best not to change the default values for this RSTP feature unless you have a good grasp of the concept. In most cases, the default values will work fine.

Note

If you are sure that there are RSTP participating bridges attached to a particular port, you should set that port's edge port status to 'NO' to prevent possible bridge loops.

Mixed STP and RSTP Networks

RSTP IEEE 802.1w is fully compliant with STP IEEE 802.1d. Your network can consist of bridges running both protocols. STP and RSTP in the same network should be able to operate together to create a single spanning tree domain.

There is no reason not to activate RSTP on an AT-8316F or an AT-8324 Switch even when all other switches are running STP. The AT-8316F or AT-8324 Switch can combine its RSTP with the STP of the other switches. An AT-8316F or AT-8324 Switch will monitor the traffic on each port for BPDU packets. Ports that receive RSTP BPDU packets will operate in RSTP while ports receiving STP BPDU packets will operate in STP.

Spanning Tree and VLANs

The spanning tree implementation on an AT-8316F or an AT-8324 Switch is a single-instance spanning tree. The switch supports just one spanning tree. You could not define multiple spanning trees.

The single spanning tree encompasses all ports on the switch. If the ports are divided into different VLANs, the spanning tree crosses the VLAN boundaries. This point can pose a problem in networks containing many VLANs that span different switches and are connected with untagged ports. What can happen is that STP will block a data link because it detects a data loop. This can cause fragmentation of your VLANs.

This issue is illustrated in Figure 34. Two VLANs, Sales and Production, span two AT-8324 Switches. Two links consisting of untagged ports interconnect the separate parts of each VLAN. If STP is activated on the switch, one of the links would be disabled. This problem can be avoided by not activating spanning tree or by connecting VLANs using tagged instead of untagged ports. (For information on tagged and untagged ports, refer to **Chapter 10, Virtual LANs** on page 117.

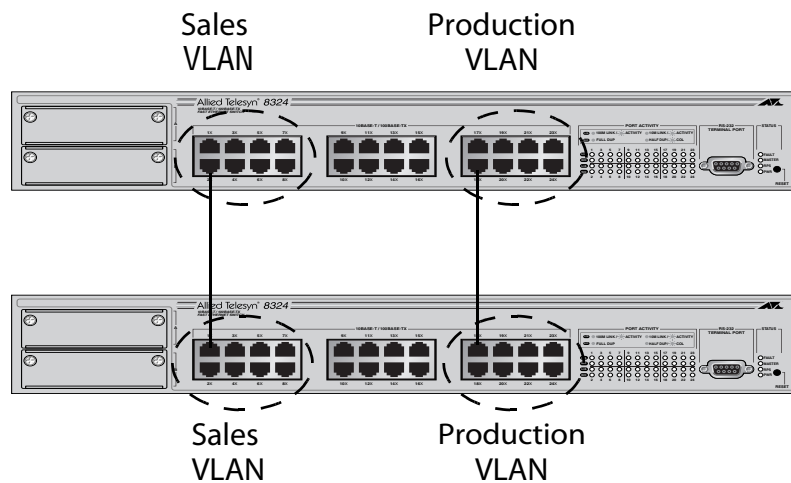


Figure 34 VLAN Fragmentation

Enabling or Disabling STP or RSTP

To enable or disable a spanning tree protocol (STP) or a rapid spanning tree protocol (RSTP), perform the following procedure:

1. From the Main Menu, type **3** to select *Spanning Tree Menu*.

The Spanning Tree Menu in Figure 35 is displayed.

```

Allied Telesyn Ethernet Switch AT-8324 - AT-S25 v2.0.2
Sales
Login Session: Manager                               Module 1 / MASTER

Spanning Tree Menu

1 - Spanning Tree Status ..... Disable
2 - Active Protocol Version ..... RSTP
3 - STP Configuration
4 - RSTP Configuration

S - Save Configuration changes
R - Return to Previous Menu

Enter your selection? _

```

Figure 35 Spanning Tree Menu

2. To select the spanning tree protocol version, type **2** to select STP or RSTP as *Active Protocol Version*.

The following prompt is displayed:

```
Enter new value (S-STP, R-RSTP):
```

3. Type **S** to select STP or type **R** to select RSTP.
4. To enable or disable the selected protocol version, type **1** to select *Spanning Tree Status*.

The following prompt is displayed.

```
Enter new value (E-Enable, D-Disable):
```

5. Type **E** to enable the RSTP or **D** to disable it. The default is disabled.
6. If you enable the STP, go to **Configuring STP** on page 105.
7. If you enable the RSTP, go to **Configuring RSTP** on page 110.

STP and RSTP Parameters

Since both STP and RSTP are sharing the same parameters; instead of having them listed by sections in this chapter, they are now listed in the Table 9 below:

Note

Any changes made to the common parameters will be take effect on both protocols such as: Bridge Priority, Bridge Hello Time,...."

Table 9 STP and RSTP Parameters

PARAMETER	DESCRIPTION
Force Version	<p>This selection determines whether the bridge will operate with RSTP or in an STP-compatible mode.</p> <ul style="list-style-type: none"> • If you select <i>RSTP</i>, the bridge will operate all ports in RSTP, except for those ports that receive STP BPDU packets. • If you select <i>Force STP Compatible</i>, the bridge will operate in RSTP, using the RSTP parameter settings, but it will send only STP BPDU packets out the ports.
Bridge Priority	<p>The priority number for the bridge. This number is used in determining the root bridge for RSTP. The bridge with the lowest priority number is selected as the root bridge. If two or more bridges have the same priority value, the bridge with the numerically lowest MAC address becomes the root bridge. When a root bridge goes off-line, the bridge with the next priority number automatically takes over as the root bridge.</p> <p>This parameter has a range of from 0 (zero) to 61,440 in increments of 4096, with 0 being the highest priority. For a list of the increments, refer to Table 6, Bridge Priority Value Increments on page 94.</p>
Bridge Hello Time	<p>The time interval between generating and sending configuration messages by the bridge.</p> <p>This parameter has a range of from 1 to 10 seconds. The default is 2 seconds.</p>
Bridge Forwarding	<p>The waiting period before a bridge changes to a new state, for example, becomes the new root bridge after the topology changes. If the bridge transitions too soon, not all links may have yet adapted to the change, possibly resulting in a network loop.</p> <p>This parameter has a range of from 4 to 30 seconds. The default is 15 seconds.</p>

Table 9 STP and RSTP Parameters

PARAMETER	DESCRIPTION
Bridge Max Age	<p>The length of time after which stored bridge protocol data units (BPDUs) are deleted by the bridge. All bridges in a bridged LAN use this aging time to test the age of stored configuration messages called BPDUs.</p> <p>For example, if you use the default 20, all bridges delete current configuration messages after 20 seconds. This parameter can be from 6 to 40 seconds. The default is 20 seconds.</p> <p>In selecting a value for maximum age, the following must be observed:</p> <ul style="list-style-type: none"> • MaxAge must be more then $[2 \times (\text{HelloTime} + 1)]$ • MaxAge must be less then $[2 \times (\text{ForwardingDelay} - 1)]$
Bridge Identifier	<p>The MAC address of the bridge. The bridge identifier is used as a tie breaker in the selection of the root bridge when two or more bridges have the same bridge priority value.</p> <p>This value cannot be changed.</p>
Root Bridge	<p>The MAC address of the bridge functioning as the root bridge in the spanning tree domain. This value is for viewing purposes only and cannot be changed.</p>
Root Priority	<p>The priority number of the root bridge. This value is for viewing purposes only and cannot be changed.</p>
Port Priority or Priority	<p>This parameter is used as a tie breaker when two or more ports are determined to have equal costs to the root bridge. The range is 0 to 240 in increments of 16. The default value is 8 (priority value 128).</p> <p>For a list of the increments, refer to Table 8, Port Priority Value Increments on page 96.</p>
Port Cost or Cost	<p>The rapid spanning tree algorithm uses the cost parameter to decide which port provides the lowest cost path to the root bridge.</p> <p>For an explanation of this parameter, refer to Table 7, Auto-Detect Port Costs on page 95.</p>
Point-to-Point or P2P	<p>This parameter defines whether the port is functioning as a point-to-point port.</p> <p>This parameter only applies to RSTP. For an explanation of this parameter, refer to Point-to-Point Ports and Edge Ports on page 98.</p>

Table 9 STP and RSTP Parameters

PARAMETER	DESCRIPTION
Edge Port	<p>This parameter defines whether the port is functioning as an edge port.</p> <p>This parameter only applies to RSTP. For an explanation of this parameter, refer to Point-to-Point Ports and Edge Ports on page 98.</p>
Port	The port number.
State	The current state of the selected port.
Role	<p>The current role of the selected port.</p> <p>The settings for this parameter are:</p> <ul style="list-style-type: none"> • Root Port • Alternate • Designated • Backup
Version	<p>The version of the BPDU.</p> <p>The settings for this parameter are:</p> <ul style="list-style-type: none"> • STP • RSTP

Configuring STP

This section contains the following procedures:

- ❑ **Configuring a Bridge's STP Settings** on page 105
- ❑ **Configuring a Port's STP Settings** on page 107

Configuring a Bridge's STP Settings

This section contains the procedure for configuring a bridge's STP settings.



Caution

The default STP parameters are adequate for most networks. Changing them without prior experience and an understanding of how STP works might have a negative effect on your network. You should consult the IEEE 802.1d standard before changing any of the STP parameters.

1. From the Main Menu, type **3** to select *Spanning Tree Menu*.
The Spanning Tree Menu in Figure 35 on page 101 is displayed.
2. From the Spanning Tree Menu, type **2** to select *Active Protocol Version*.
The following prompt is displayed:

Enter new value (S-STP, R-RSTP):

3. Type **S** to select *STP*.
4. Type **3** to select *STP Configuration*.
The STP Menu in Figure 36 is displayed.

```

Allied Telesyn Ethernet Switch AT-8324 - AT-S25 v2.0.2
Sales
Login Session: Manager                               Module 1 / MASTER

                                STP Menu

1 - Bridge Priority ..... 32768
2 - Bridge Hello Time ..... 2
3 - Bridge Forwarding ..... 15
4 - Bridge Max Age ..... 20
5 - Bridge Identifier ..... 00:00:00:00:00:00

P - STP Port Parameters
D - Reset STP to Defaults

S - Save Configuration changes
R - Return to Previous Menu

Enter your selection?

```

Figure 36 STP Menu

5. Enter or modify the bridge STP settings as desired.

For description of the parameters displayed in this window, refer to Table 9, **STP and RSTP Parameters** on page 102.

6. After adjusting the parameters, type **S** to select *Save Configuration changes*.

Changes to the parameters take effect immediately on the switch.

Note

The aging time for BPDUs is different from the aging time used by the MAC address table.

7. To reset a bridge's STP settings to the default settings, type **D**.
8. To change the STP port settings, go to **Configuring a Port's STP Settings** on page 107.

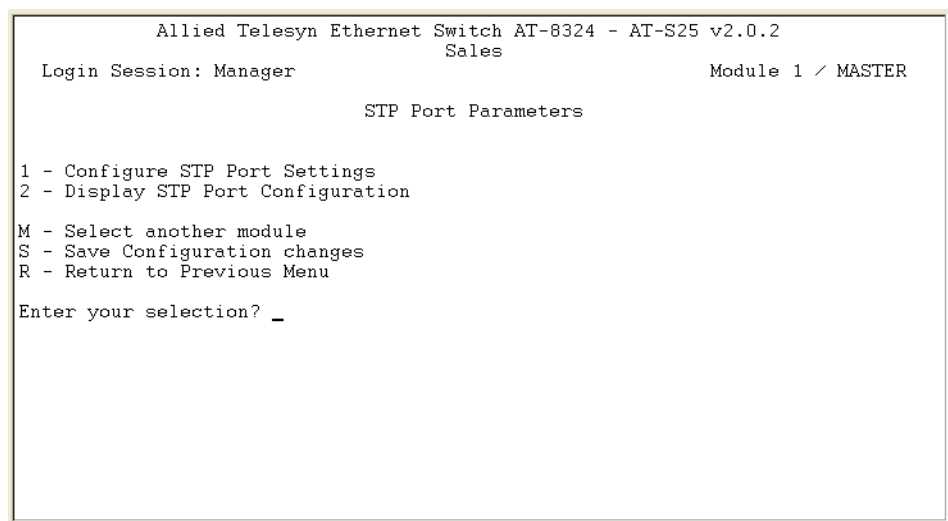
Configuring a Port's STP Settings

To adjust a port's STP parameters, perform the following procedure:

1. From the Spanning Tree Menu, type **2** to select *Active Protocol Version*.
The following prompt is displayed:

```
Enter new value (S-STP, R-RSTP):
```

2. Type **S** to select *STP*.
3. Type **3** to select *STP Configuration*.
The STP Menu in Figure 36 on page 105 is displayed.
4. From the STP Menu, type **P** to select *STP Port Parameters*.
The STP Port Parameters menu in Figure 37 is displayed.



```

Allied Telesyn Ethernet Switch AT-8324 - AT-S25 v2.0.2
Sales
Login Session: Manager                               Module 1 / MASTER

                STP Port Parameters

1 - Configure STP Port Settings
2 - Display STP Port Configuration
M - Select another module
S - Save Configuration changes
R - Return to Previous Menu

Enter your selection? _

```

Figure 37 STP Port Parameters Menu

5. From the STP Port Parameters window, type **M** if you wish to select a module other than the one currently displayed.

The prompt message is displayed:

```
Select Module ID: [1 to 8] ->
```

6. Enter the ID of the module you wish to select, and press the Enter key.
7. From the STP Port Parameters window, type **1** to select *Configure RSTP Port Settings*.

The following prompt is displayed:

```
Start Port to configure [1 - 24] ->
```

8. Enter the number of the port you wish to configure. To configure a range of ports, enter the first port of the range. Press the Enter key.

The following prompt is displayed:

End Port to Configure [1 - 24] ->

- ☐ To configure just one port, enter the same port number here as you entered in the previous step.
- ☐ To configure a range of ports, enter the last port of the range.

9. Press the Enter key.

The Configure STP Port Settings menu in Figure 38 is displayed.

```

Allied Telesyn Ethernet Switch AT-8324 - AT-S25 v2.0.2
Sales
Login Session: Manager                               Module 1 / MASTER

Configure STP Port Settings

Configuring Ports 1 to 6
1 - Port Priority ..... 128
2 - Port Cost ..... Automatic-Update.

S - Save Configuration changes
R - Return to Previous Menu

Enter your selection? _

```

Figure 38 Configure STP Port Settings Menu

10. Enter or modify a port's STP settings as desired.

For description of the parameters displayed in this window, refer to Table 9, **STP and RSTP Parameters** on page 102.

11. After adjusting the parameters, type **S** to select *Save Configuration changes*.

Note

A change to the port priority parameter takes effect immediately. A change to the port cost value requires you to reset the switch. A new port cost value is not implemented until the unit is reset.

Displaying Port's STP Status and Setting

To display a port's STP status and settings, perform the following procedure:

1. From the Spanning Tree Menu, type **2** to select *Active Protocol Version*.

The following prompt is displayed:

```
Enter new value (S-STP, R-RSTP):
```

2. Type **S** to select *STP*.
3. Type **3** to select *STP Configuration*. The STP Menu in Figure 36 on page 105 is displayed.
4. From the STP Menu, type **P** to select *STP Port Parameters*. The STP Port Parameters window in Figure 37 on page 107 is displayed.
5. From the STP Port Parameters window, type **M** if you wish to select a module other than the one currently displayed.

The prompt message is displayed:

```
Select Module ID: [1 to 8] ->
```

6. Enter the ID of the module you wish to select, and press the Enter key.
7. In the STP Port Parameters window, type **2** to select *Display STP Port Configuration*. The Display STP Port Configuration window in Figure 39 is displayed.

```

Allied Telesyn Ethernet Switch AT-8324 - AT-S25 v2.0.2
Sales
Login Session: Manager
Module 1 / MASTER

Display STP Port Configuration

Port      State      Cost      Priority
-----
1         Disabled   Auto-Update 128
2         Disabled   20000       64
3         Disabled   Auto-Update 128
4         Disabled   Auto-Update 128
5         Disabled   Auto-Update 128
6         Disabled   Auto-Update 128
7         Disabled   Auto-Update 128
8         Disabled   Auto-Update 128

N - Next Page
U - Update Display
R - Return to Previous Menu

Enter your selection? _

```

Figure 39 Display STP Port Configuration Window

The parameters displayed in this window are for viewing purposes only. For description of the parameters, refer to Table 9, **STP and RSTP Parameters** on page 102.

Configuring RSTP

This section contains the following procedures:

- ❑ **Configuring a Bridge's RSTP Settings** on page 110
- ❑ **Configuring a Port's RSTP Settings** on page 111

Configuring a Bridge's RSTP Settings

This section contains the procedure for configuring a bridge's RSTP settings.



Caution

The default RSTP parameters are adequate for most networks. Changing them without prior experience and an understanding of how RSTP works might have a negative effect on your network. You should consult the IEEE 802.1w standard before changing any of the RSTP parameters.

1. From the Main Menu, type **3** to select *Spanning Tree Menu*.
The Spanning Tree Menu in Figure 35 on page 101 is displayed.
2. From the Spanning Tree Menu, type **2** to select *Active Protocol Version*.
The following prompt is displayed:

Enter new value (S-STP, R-RSTP):

3. Type **R** to select *RSTP*.
4. Type **4** to select *RSTP Configuration*.

The RSTP Menu window in Figure 39 is displayed.

```

Allied Telesyn Ethernet Switch AT-8324 - AT-S25 v2.0.2
Sales
Login Session: Manager                               Module 1 / MASTER

RSTP Menu

1 - Force Version ..... RSTP
2 - Bridge Priority ..... 32768
3 - Bridge Hello Time ..... 2
4 - Bridge Forwarding ..... 15
5 - Bridge Max Age ..... 20
6 - Bridge Identifier ..... 00:00:00:00:00:00

P - RSTP Port Parameters
D - Reset RSTP to Defaults

S - Save Configuration changes
R - Return to Previous Menu

Enter your selection? _

```

Figure 40 RSTP Menu

5. Enter or modify the parameters in the RSTP Menu window as desired.
For description of the parameters displayed in this window, refer to Table 9, **STP and RSTP Parameters** on page 102.
6. After adjusting the parameters, type **S** to select *Save Configuration changes*.

Changes to the parameters take effect immediately on the switch.

Note

The aging time for BPDUs is different from the aging time used by the MAC address table.

7. To reset a bridge's RSTP settings to the default settings, type **D**.
8. To change the RSTP port settings, go to the next procedure.

Configuring a Port's RSTP Settings

To adjust a port's RSTP parameters, perform the following procedure:

1. From the Main Menu, type **3** to select *Spanning Tree Menu*.
2. From the Spanning Tree Menu, type **2** to select *Active Protocol Version*.

The following prompt is displayed:

```
Enter new value (S-STP, R-RSTP):
```

3. Type **R** to select *RSTP*.
4. Type **4** to select *RSTP Configuration*.
5. From the RSTP Configuration menu, type **P** to select *RSTP Port Parameters*.

The RSTP Port Parameters menu in Figure 41 on page 111 is displayed.

```

Allied Telesyn Ethernet Switch AT-8324 - AT-S25 v2.0.2
Sales
Login Session: Manager                               Module 1 / MASTER

RSTP Port Parameters

1 - Configure RSTP Port Settings
2 - Display RSTP Port Configuration
3 - Display RSTP Port State

M - Select another module
S - Save Configuration changes
R - Return to Previous Menu

Enter your selection? _

```

Figure 41 RSTP Port Parameters Menu

6. From the RSTP Port Parameters window, type **M** if you wish to select a module other than the one currently displayed.

The prompt message is displayed:

```
Select Module ID: [1 to 8] ->
```

7. Enter the ID of the module you wish to select, and press the Enter key.
8. From the RSTP Port Parameters window, type **1** to select *Configure RSTP Port Settings*.

The following prompt is displayed:

```
Start Port to configure [1 - 24] ->
```

9. Enter the number of the port you wish to configure. To configure a range of ports, enter the first port of the range. Press the Enter key.

The following prompt is displayed:

```
End Port to Configure [1 - 24] ->
```

- ☐ To configure just one port, enter the same port number here as you entered in the previous step.
 - ☐ To configure a range of ports, enter the last port of the range.
10. Press the Enter key.

The Configure RSTP Port Settings menu in Figure 42 on page 112 is displayed.

```

Allied Telesyn Ethernet Switch AT-8324 - AT-S25 v2.0.2
Sales
Login Session: Manager                               Module 1 / MASTER

                Configure RSTP Port Settings

Configuring Ports 1 to 6
1 - Port Priority ..... 128
2 - Port Cost ..... Automatic-Update.
3 - Point-To-Point ..... Auto Detect
4 - Edge Port ..... Yes

S - Save Configuration changes
R - Return to Previous Menu
Enter your selection? _

```

Figure 42 Configure RSTP Port Settings Menu

11. Enter or modify the parameters in the window as desired.

For description of the parameters displayed in this window, refer to Table 9, **STP and RSTP Parameters** on page 102.

12. After making your changes, type **S** to select *Save Configuration changes*.

Note

All changes to a port's RSTP settings, with the exception of port cost, are activated immediately. A change to the port cost value requires you to reset the switch. A new port cost value is not implemented until the unit is reset.

Displaying Port's RSTP Status and Settings

Unlike the information displayed for STP, the RSTP status and settings information are listed separated in the AT-S25 software, under the following menus:

- ☐ Display RSTP Port Settings
- ☐ Display RSTP Port State

Displaying a Port's RSTP Settings

To display a port's RSTP settings, perform the following procedure:

1. From the Spanning Tree Menu, type **2** to select *Active Protocol Version*. The following prompt is displayed:

Enter new value (S-STP, R-RSTP) :

2. Type **R** to select *RSTP*.
3. Type **4** to select *RSTP Configuration*.

The RSTP Menu in Figure 40 on page 110 is displayed.

4. From the RSTP Menu, type **P** to select *RSTP Port Parameters*.

The RSTP Port Parameters window in Figure 37 on page 107 is displayed.

5. From the RSTP Port Parameters window, type **M** if you wish to select a module other than the one currently displayed.

The prompt message is displayed:

Select Module ID: [1 to 8] ->

6. Enter the ID of the module you wish to select, and press the Enter key.
7. In the RSTP Port Parameters window, type **2** to select *Display RSTP Port Settings*.

The Display RSTP Port Configuration window in Figure 39 is displayed.

```

Allied Telesyn Ethernet Switch AT-8324 - AT-S25 v2.0.2
Sales
Login Session: Manager
Module 1 / MASTER

Display RSTP Port Configuration

Port      Edge-Port    Point-to-Point    Cost              Priority
-----
1      Yes      Auto Detect      Auto Update      128
2      Yes      Auto Detect      20000            64
3      Yes      Auto Detect      Auto Update      128
4      Yes      Auto Detect      Auto Update      128
5      Yes      Auto Detect      Auto Update      128
6      Yes      Auto Detect      Auto Update      128
7      Yes      Auto Detect      Auto Update      128
8      Yes      Auto Detect      Auto Update      128

N - Next Page
U - Update Display
R - Return to Previous Menu

Enter your selection? _

```

Figure 43 Display RSTP Port Configuration Window

The parameters displayed in this window are for viewing purposes only. For description of the parameters, refer to Table 9, **STP and RSTP Parameters** on page 102.

Displaying a Port's RSTP Status

To display a port's RSTP status, perform the following procedure:

1. From the Spanning Tree Menu, type **2** to select *Active Protocol Version*. The following prompt is displayed:

Enter new value (S-STP, R-RSTP):

2. Type **R** to select *RSTP*.
3. Type **4** to select *RSTP Configuration*.

The RSTP Menu in Figure 40 on page 110 is displayed.

4. From the RSTP Menu, type **P** to select *RSTP Port Parameters*.

The RSTP Port Parameters window in Figure 41 on page 111 is displayed.

5. From the RSTP Port Parameters window, type **M** if you wish to select a module other than the one currently displayed.

The prompt message is displayed:

Select Module ID: [1 to 8] ->

6. Enter the ID of the module you wish to select, and press the Enter key.

7. In the RSTP Port Parameters window, type **3** to select *Display RSTP Port State*.

The Display RSTP Port State window in Figure 44 is displayed.

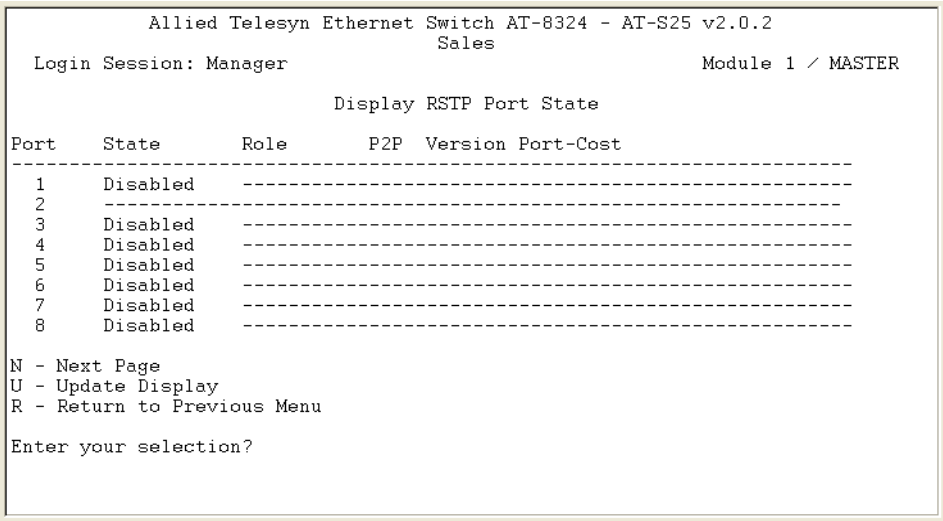


Figure 44 Display RSTP Port State Window

The parameters displayed in this window are for viewing purposes only. For description of the parameters, refer to Table 9, **STP and RSTP Parameters** on page 102.

Chapter 9

Virtual LANs

This chapter contains basic information about virtual LANs (VLANs). It also explains how to create, modify, and delete VLANs from a local or Telnet management session. This chapter also describes the Basic VLAN mode and how you could change a switch's VLAN operating mode.

This chapter contains the following sections:

- ❑ **VLAN Overview** on page 118
- ❑ **Port-based VLAN Overview** on page 120
- ❑ **Tagged VLAN Overview** on page 125
- ❑ **Basic VLAN Mode Overview** on page 129
- ❑ **Creating a Port-based or Tagged VLAN** on page 130
- ❑ **Modifying a VLAN** on page 134
- ❑ **Displaying VLAN Information** on page 137
- ❑ **Deleting a VLAN** on page 138
- ❑ **Deleting All VLANs** on page 140
- ❑ **Displaying PVIDs** on page 141
- ❑ **Specifying a Management VLAN** on page 143
- ❑ **Switching the VLAN Mode** on page 145

VLAN Overview

A VLAN is a group of ports on an Ethernet switch that form a logical Ethernet segment. The ports of a VLAN form an independent traffic domain where the traffic generated by the nodes of a VLAN remains within the VLAN.

With VLANs, you could segment your network through the switch's management software and so be able to group nodes with related functions into their own separate, logical LAN segments. These VLAN groupings can be based on similar data needs or security requirements. For example, you could create separate VLANs for the different departments in your company, such as one for Sales and another for Production.

VLANs offer several important benefits:

- ☐ Improved network performance

Network performance often suffers as networks grow in size and data traffic increases. The more nodes on each LAN segment vying for bandwidth, the more likely overall network performance will decrease.

VLANs improve network performance by restricting data traffic within a VLAN. The nodes of a VLAN receive traffic only from nodes of the same VLAN. This reduces the need for nodes to handle traffic not destined for them. It also frees up bandwidth within all the logical workgroups.

Additionally, since each VLAN constitutes a separate broadcast domain, broadcast traffic remains within the VLAN. This too can improve overall network performance.

- ☐ Increased security

Since data traffic generated by a node in a VLAN is restricted only to the other nodes of the same VLAN, VLANs can be used to control the flow of data in your network and prevent data from flowing to unauthorized end nodes.

- ☐ Simplified network management

VLANs can also simplify network management. Before the advent of VLANs, physical changes to the network often had to be made at the switches in the wiring closets. For example, if an employee changed departments, changing the employee's LAN segment assignment might require a change to the wiring at the switches.

But with VLANs, you could change the LAN segment assignment of an end node connected to the switch through the switch's AT-S25 management software. VLAN memberships can be changed any time through the management software without moving the workstations physically, or having to change group memberships by moving cables from one switch port to another.

Additionally, a virtual LAN can span more than one switch. This means that the end nodes of a VLAN do not need to be connected to the same switch and so are not restricted to being in the same physical location.

The AT-8300 Series switches support the following types of VLANs:

- ☐ Port-based VLANs
- ☐ Tagged VLANs

These VLANs are described in the following sections.

Port-based VLAN Overview

As explained in the **VLAN Overview** section earlier in this chapter, a VLAN consists of a group of ports on one or more Ethernet switches that form an independent traffic domain. Traffic generated by the end nodes of a VLAN remains within the VLAN and does not cross over to the end nodes of other VLANs unless there is an interconnection device, such as a router or Layer 3 switch.

A port-based VLAN is a group of ports on a Fast Ethernet Switch that form a logical Ethernet segment. Each port of a port-based VLAN can belong to only one VLAN at a time.

A port-based VLAN can have as many or as few ports as desired. The VLAN can consist of all the ports on an Ethernet switch, or just a few ports. A port-based VLAN also can span switches and consist of ports from multiple Ethernet switches.

Note

The AT-8316F or AT-8324 Switch is pre-configured with one port-based VLAN. All ports on the switch are members of this VLAN, called the Default VLAN.

The parameters that make up a port-based VLAN are described in the following sections.

VLAN Name To create a port-based VLAN, you must give it a name. The name should reflect the function of the network devices that are be members of the VLAN. Examples include Sales, Production, and Engineering.

VLAN Identifier Each VLAN in a network must have a unique number assigned to it. This number is called the VLAN identifier (VID). This number uniquely identifies a VLAN in the switch and the network.

If a VLAN consists only of ports located on one physical switch in your network, you would assign it a VID unique from all other VLANs in your network.

If a VLAN spans multiple switches, then the VID for the VLAN on the different switches must be the same. In this manner, the switches are able to recognize and forward frames belonging to the same VLAN even though the VLAN spans multiple switches.

For example, if you had a port-based VLAN titled Marketing that spanned three AT-8324 Switches, you would assign the Marketing VLAN on each switch the same VID.

You could assign this number manually or allow the management software to do it automatically. If you allow the management software to do it automatically, it will simply select the next available VID. This is acceptable when you are creating a new, unique VLAN.

If you are creating a VLAN on a switch that will be part of a larger VLAN that spans several switches, then you will need to assign the number yourself so that the VLAN has the same VID on all switches.

Untagged Ports

Naturally, you need to specify which ports on the switch are to be members of a port-based VLAN. Ports in a port-based VLAN are referred to as *untagged ports* and the frames received on the ports as *untagged frames*. The names derive from the fact that the frames received on a port will not contain any information that indicates VLAN membership, and that VLAN membership will be determined solely by the port's PVID. (There is another type of VLAN where VLAN membership is determined by information within the frames themselves, rather than by a port's PVID. This type of VLAN is explained in **Tagged VLAN Overview** on page 125.)

A port on a switch can be an untagged member of only one port-based VLAN at a time. An untagged port cannot be assigned to two port-based VLANs simultaneously.

Port VLAN Identifier

Each port in a port-based VLAN must have a port VLAN identifier (PVID). The switch associates a frame to a port-based VLAN by the PVID assigned to the port on which the frame is received, and forwards the frame only to those ports with the same PVID. Consequently, all ports of a port-based VLAN must have the same PVID. Additionally, the PVID of the ports in a VLAN must match the VLAN's VID.

For example, assume that you were creating a port-based VLAN on a switch and you had assigned the VLAN the VID 5. Consequently, the PVID for each port in the VLAN also needs to be assigned the value 5.

Some switches and switch management programs require that you assign the PVID value for each port manually. However, the AT-S25 management software performs this task automatically. The software automatically assigns a PVID to a port, making it identical to the VID of the VLAN to which the port is an untagged member.

General Rules to Creating a Port-based VLAN

Below is a summary of the general rules to observe when creating a port-based VLAN.

- ❑ Each port-based VLAN must be assigned a unique VID. If a particular VLAN spans multiple switches in a stack, each port of the VLAN on the different switches must be assigned the same VID.

- ☐ A port can be an untagged member of only one port-based VLAN at a time.
- ☐ Each port must be assigned a PVID. This value must be the same for all ports in a port-based VLAN and it must match the VLAN's VID. This value is assigned automatically by the AT-S25 management software.
- ☐ If there are end nodes in different VLANs that need to communicate with each other, a router or Layer 3 switch is required to interconnect the VLANs.

Drawbacks to Port-based VLANs

There are several drawbacks to port-based VLANs:

- ☐ It is not easy to share network resources, such as servers and printers, across multiple VLANs. A router or Layer 3 switch must be added to the network to provide a means for interconnecting the port-based VLANs.
- ☐ The introduction of a router into your network could create security issues from unauthorized access to your network.
- ☐ A VLAN that spans several stacks of switches will require a port on each switch for the interconnection of the various parts of the VLAN. For example, a VLAN that spans three switches would require one port on each switch to interconnect the various sections of the VLAN. In network configurations where there are many individual VLANs that span switches, many ports can end up being used ineffectively just to interconnect the various VLANs.

Port-based VLAN Example

Figure 45 is an example of two port-based VLANs that span an AT-8316F or an AT-8324 Switch and one AT-8024 Switch.

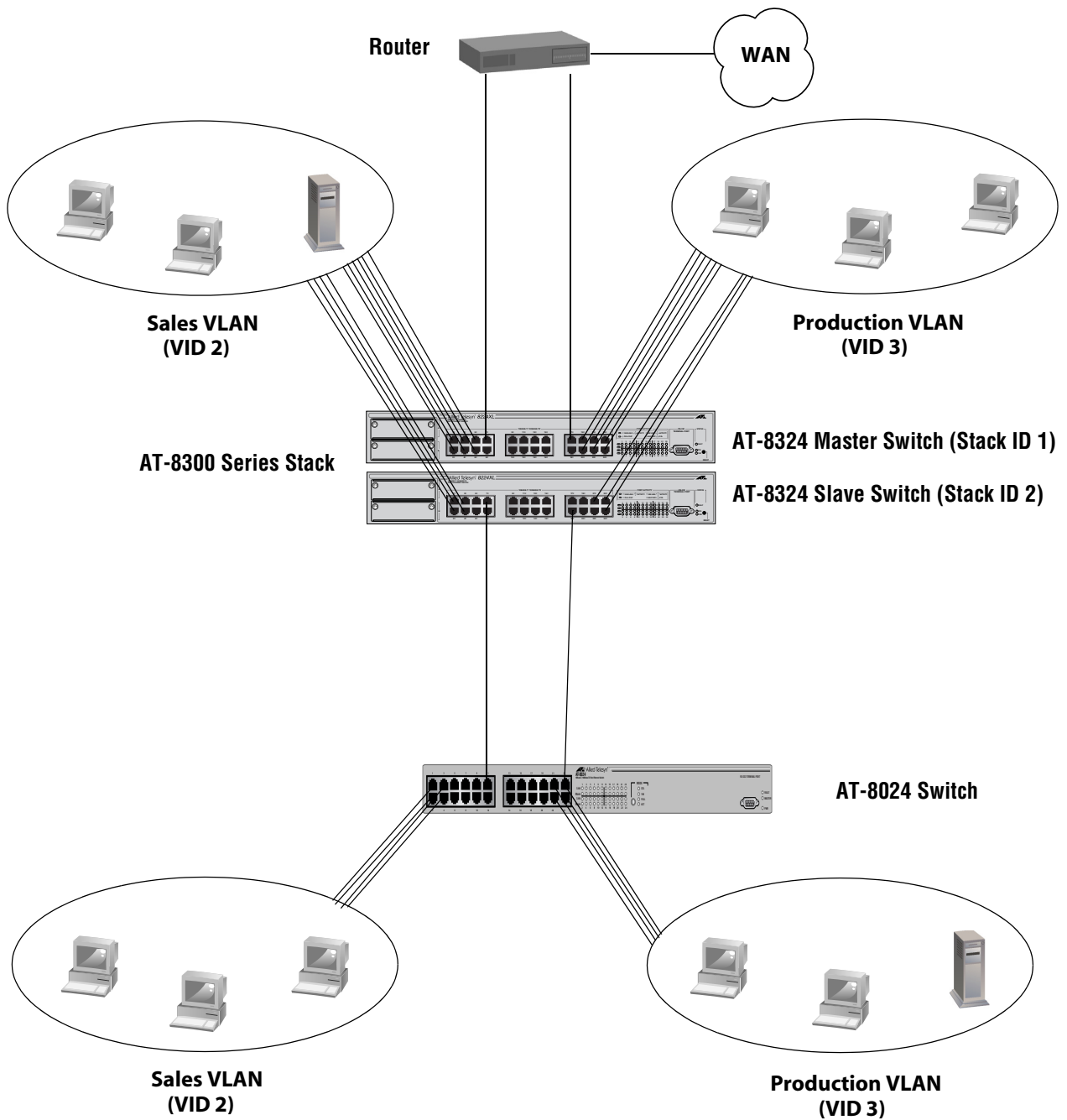


Figure 45 Port-based VLAN Example

Table 10 lists the ports assignments for the Sales and Production VLANs:

Table 10 Port Assignments of the Port-based VLAN Example

Switch	Sales VLAN (VID 2)	Production VLAN (VID 3)
AT-8324 Switch (Master)	Ports 1 - 7 (PVID 2)	Ports 17, 19 - 24 (PVID 3)
AT-8324 Switch (Slave)	Ports 1 - 4, 8 (PVID 2)	Ports 20, 21, 23, 24 (PVID 3)
AT-8024 Switch	Ports 1 - 4, 7 (PVID 2)	Ports 19, 21 - 24 (PVID 3)

Each VLAN is briefly summarized below:

- ❑ Sales VLAN — This VLAN has been assigned a VID of 2 and the ports, correspondingly, have been automatically assigned a PVID also of 2. This VLAN spans the AT-8300 Series stack and the AT-8024 Switch. Ports 1 to 6 on the Master AT-8324 Switch and ports 1 to 4 on the Slave switch are connected to workstations and a server. Port 7 on the Master switch is connected to the router, which gives the Sales VLAN access to the Production VLAN and also to the WAN. Port 8 on the Slave switch is functioning as a direct link to the second part of the Sales VLAN, located on the AT-8024 Switch.
- ❑ Production VLAN — This VLAN has been assigned a VID of 3 and the ports a PVID of 3. Ports 19 to 24 on the Master AT-8324 Switch and ports 21, 23, and 24 on the Slave switch are connected to workstations. Port 17 on the Master switch is connected to a router for interconnection to the Sales VLAN and the WAN, and port 20 on the Slave switch is connected to the AT-8024 Switch to interconnect the two parts of the Production VLAN.

Tagged VLAN Overview

The second type of VLAN supported by the AT-8300 Series switch is the *tagged VLAN*. VLAN membership in a tagged VLAN is determined by information within the frames that are received on a port. This contrasts to a port-based VLAN, where the PVIDs assigned to the ports determine VLAN membership.

The VLAN information within an Ethernet frame is referred to as a *tag* or *tagged header*. A tag, which follows the source and destination addresses in a frame, contains the VID of the VLAN to which the frame belongs (IEEE 802.3ac standard). As explained earlier in this chapter in **VLAN Identifier** on page 120, this number uniquely identifies each VLAN in a network.

When a switch receives a frame with a VLAN tag, referred to as a *tagged frame*, the switch forwards the frame only to those ports that share the same VID.

A port to receive or transmit tagged frames is referred to as a *tagged port*. Any network device connected to a tagged port must be IEEE 802.1Q-compliant. This is the standard that outlines the requirements and standards for tagging. The device must be able to process the tagged information on received frames and add tagged information to transmitted frames.

The benefit of a tagged VLAN is that the tagged ports within the VLAN can belong to more than one VLAN at one time. This can greatly simplify the task of adding shared devices to the network. For example, a server can be configured to accept and return packets from many different VLANs simultaneously.

Tagged VLANs are also useful where multiple VLANs span across switches. You could use one port per switch for connecting all VLANs on the switch to another switch.

The IEEE 802.1Q standard deals with how this tagging information is used to forward the traffic throughout the switch. The handling of frames tagged with VIDs coming into a port is straightforward. If the incoming frame's VID tag matches one of the VIDs of a VLAN that the port is a tagged member of, the frame will be accepted and forwarded to the appropriate ports. If the frame's VID does not match any of the VLANs that the port is a member of, the frame will be discarded.

The parts of a tagged VLAN are much the same as those for a port-based VLAN. They are described in the following sections.

VLAN Name	For an explanation of VLAN Name, refer to VLAN Name on page 120.
VLAN Identifier	For an explanation of VLAN Identifier, refer to VLAN Identifier on page 120.
Tagged and Untagged Ports	<p>You need to specify which ports will be members of the VLAN. In the case of a tagged VLAN, it will usually be a combination of both untagged ports and tagged ports. You specify which ports will be tagged and which untagged when you create the VLAN.</p> <p>An untagged port, whether a member of a port-based VLAN or a tagged VLAN, can be in only one VLAN at a time. However, a tagged port can be a member of more than one VLAN. A port can also be an untagged member of one VLAN and a tagged member of different VLANs, simultaneously.</p>
Port VLAN Identifier	<p>As explained earlier in the discussion on port-based VLANs, the management software automatically assigns a PVID to each port when a port is made a member of a VLAN. The PVID is always identical to the VLAN's VID, and that in a port-based VLAN packets are forwarded based on the PVID.</p> <p>Since a tagged port determines VLAN membership by examining the tagged header within the frames that it receives, there would seem to be no need for a PVID. But actually there is. The PVID is used if a tagged port receives an untagged frame (that is, a frame without any tagged information). The port will forward the frame based on the port's PVID. But this is only in cases where untagged frames arrive on tagged ports. Otherwise, the PVID of a port is ignored on a tagged port.</p>
General Rules to Creating a Tagged VLAN	<p>Below is a summary of the rules to observe when creating a tagged VLAN.</p> <ul style="list-style-type: none"><input type="checkbox"/> The AT-8300 Series switch can support up to 255 VLANs.<input type="checkbox"/> Each tagged VLAN must be assigned a unique VID. If a particular VLAN spans multiple switches, each part of the VLAN on the different switches must be assigned the same VID.<input type="checkbox"/> A tagged port can be a member of multiple VLANs.<input type="checkbox"/> An untagged port can be an untagged member of only one VLAN at a time.<input type="checkbox"/> Each tagged port is required to have a PVID. If the port's untagged membership is to be removed from a port, the switch will automatically set the PVID to 'one'. This may not be obvious unless you view the port status or reboot the switch.

Tagged VLAN Example

Figure 46 is an example of a network that uses tagged ports in two tagged VLANs to share network devices.

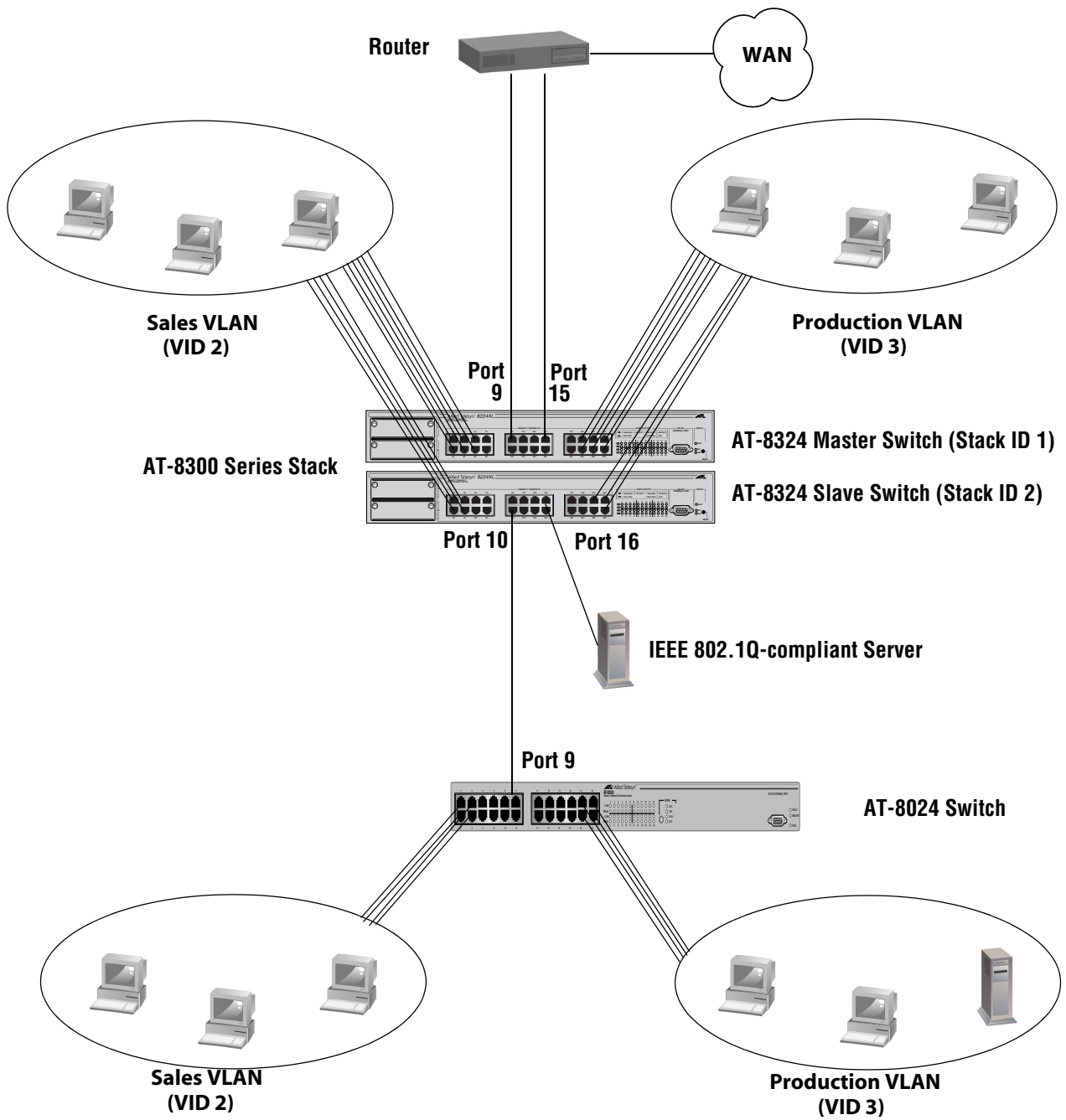


Figure 46 Tagged VLAN Example

The port assignments for the VLANs are as follows:

	Sales VLAN (VID 2)		Production VLAN (VID 3)	
	Untagged Ports	Tagged Ports	Untagged Ports	Tagged Ports
AT-8316F or AT-8324 Switch				
AT-8324 Switch (Master)	1 to 6, 9 (PVID 2)		19 - 24, 15 (PVID 3)	
AT-8324 Switch (Slave)	1 - 4 (PVID 2)	10, 16	22 - 24 (PVID 3)	10, 16
AT-8024 Switch	1 - 4 (PVID 2)	9	21 - 24 (PVID 3)	9

This configuration is similar to the port-based VLAN example earlier in this appendix, but untagged ports have replaced several connections. The changes are noted below:

- ❑ Uplink to the AT-8024 Switch - In the earlier port-based VLAN example, the Sales and Production VLANs in the AT-8300 Series stack had dedicated connections to their corresponding VLAN in the AT-8024 Switch. These connections have been replaced with one connection. Port 10 on the AT-8324 Slave switch has been made a tagged member of both VLANs, as has port 9 on the AT-8024 Switch. The connection between the ports now carries traffic for both VLANs. However, frame traffic is restricted to its respective VLAN member ports.
- ❑ Uplink to an IEEE 802.1Q-compliant server - Port 16 on the AT-8324 Slave switch has been connected to an IEEE 802.1Q-compliant server, meaning the device is capable of handling tagged frames. By designating it as a tagged port of both the Sales and Production VLANs, end-nodes from either VLAN can access the resource without having to pass through a router or Layer 3 switch.

Basic VLAN Mode Overview

The Fast Ethernet switches support a special VLAN configuration referred to as Basic VLAN Mode. When the Basic VLAN Mode is activated, frames are forwarded based solely on MAC addresses. All VLAN information, including PVIDs assigned to ports and VLAN tags in tagged frames, is ignored. Tagged frames are analyzed only for priority level.

Packets are passed through the switch unchanged. Tagged and untagged frames exit the switch the same as they entered, either tagged or untagged, regardless of the type of ports on which the frames are received and transmitted.

You should be aware of the following before you activate the Basic VLAN mode:

- ☐ You cannot create or modify port-based or tagged VLANs when the Basic VLAN Mode is activated.
- ☐ Any pre-existing port-based or tagged VLANs are retained in the event you later disabled Basic VLAN Mode, but the VLANs are not used.

Creating a Port-based or Tagged VLAN

This procedure explains how to create a new VLAN. A new VLAN automatically spans all of the switches in a stack, making it unnecessary for you to have to create the VLAN on each switch in a stack. Once you have assigned the new VLAN a name and VID, you designate the ports of the VLAN from the different switches in the stack.

To create a new port-based or tagged VLAN, perform the following procedure:

1. From the Main Menu, type **2** to select *VLAN Menu*.

The VLAN Menu in Figure 47 is displayed.

```

Allied Telesyn Ethernet Switch AT-8324 - AT-S25 v2.0.2
Sales
Login Session: Manager                               Module 1 / MASTER

VLAN Menu

1 - VLAN Definition
2 - Configure Port Priorities
3 - Management VLAN ..... 1 (Default_VLAN)

S - Save Configuration changes
R - Return to Previous Menu

Enter your selection?

```

Figure 47 VLAN Menu

2. From the VLAN Menu, type **1** to select *VLAN Definition*.

The VLAN Definitions menu in Figure 48 is displayed.

```

Allied Telesyn Ethernet Switch AT-8324 - AT-S25 v2.0.2
Sales
Login Session: Manager                               Module 1 / MASTER

VLAN Definition

1 - Create VLAN
2 - Modify VLAN
3 - Delete VLAN
4 - Show All VLANs
5 - Display VLAN Ports
6 - Clear All VLANs

M - Select another module
S - Save Configuration changes
R - Return to Previous Menu

Enter your selection? _

```

Figure 48 VLAN Definition Menu

3. Type **1** to select *Create VLAN*.

The Create VLAN window is shown in Figure 49.

```

Allied Telesyn Ethernet Switch AT-8324 - AT-S25 v2.0.2
Sales
Login Session: Manager                               Module 1 / MASTER

Create VLAN

1 - VLAN Name .....
2 - VLAN ID (VID) ..... 2
3 - Tagged Ports .....
4 - Untagged Ports .....

C - Create VLAN
M - Select another module
R - Return to Previous Menu

Enter your selection? _

```

Figure 49 Create VLAN Menu

4. Type **1** to select VLAN Name.

The following prompt is displayed:

```
Enter new value ->
```

5. Enter a name for the new VLAN of from one to nineteen alphanumeric characters. The name should reflect the function of the nodes of the VLAN (for example, Sales or Accounting). The name can not contain spaces nor special characters, such as asterisks (*) or exclamation points (!). A VLAN must have a name.

A VLAN's name must be unique on the stack and must contain at least one alphabetic character. You cannot assign the same name to two VLANs in the same stack.

6. The AT-S25 management software automatically assigns the next unused VID in the stack as the VID for the new VLAN. If you want to assign the VLAN a different VID, do the following:

- a. Type **2** to select *VLAN VID*.

The following prompt is displayed:

```
Enter new value -> [2 to 2048]
```

- b. Enter a new VID for the VLAN. The range is 2 to 2048. The VID cannot already be used by another VLAN in the same stack.

7. You are now ready to begin add ports to the new VLAN. But before you do, examine the prompt in the upper right portion of the window to determine the switch module of the stack your management session is currently addressing. If there are ports on this switch you want to add as tagged or untagged ports to the VLAN, then continue with the following sub-steps. If this switch does not contain ports that you want to add to the VLAN, then go to the next step to change switches.

To add ports, do the following:

- a. To add tagged ports, type **3** to select *Tagged Ports* and enter the ports at the prompt. You can specify the ports individually (e.g., 2,5,11), as a range (e.g., 5-10), or both (e.g., 3,7,11-15,17). To specify all ports on the switch, enter ALL.
 - b. To add untagged ports, type **4** to select *Untagged Ports* and enter the ports at the prompt. You can specify the ports individually (e.g., 2,5,11), as a range (e.g., 5-10), or both (e.g., 3,7,11-15,17). To specify all ports on the switch, enter ALL.
 - c. If there are ports on other switches in the stack that you want to add to the new VLAN, change switch modules by performing Step 8. Otherwise, skip to Step 9.
8. To add ports to a new VLAN from different switch modules in a stack, you must change switches by doing the following:
 - a. Type **M** to choose *Select another module*.

The prompt message is displayed:

```
Select Module ID: [1 to 8] ->
```

- b. Enter the ID of the switch module you want to change to, and press the Enter key.
 - c. Go to Step 7 and add the ports to the VLAN.
9. Once you have added all of the ports to the new VLAN, type **C** to select *Create VLAN*.

The switch creates the new VLAN and displays the following message:

```
SUCCESS - Press any key to continue.
```

10. Press any key to continue.

The VLAN Definition menu in Figure 48 on page 130 is displayed.

11. Type **S** to select *Save Configuration changes*.

The new VLAN is now operational.

Repeat this procedure to create additional port-based and tagged VLANs.

Note

When you create a new VLAN, ports designated as untagged ports of the new VLAN are automatically removed from their current untagged VLAN assignment. For example, if you are creating a new VLAN on a switch that contains only the Default_VLAN, the ports that you specify as untagged ports of the new VLAN are automatically removed from the Default_VLAN when they are moved to the new VLAN.

Tagged ports are not removed from any current VLAN assignments because tagged ports can belong to more than one VLAN at a time.

To verify that the VLAN was created correctly, perform the procedure in **Displaying VLAN Information** on page 137.

Modifying a VLAN

This procedure explains how to change the name and the tagged and untagged ports of a VLAN. You cannot change a VLAN's VID.

Note

To modify a VLAN, you need to know its VID. To view VLAN VIDs, refer to the procedure **Displaying VLAN Information** on page 137.

To modify a VLAN, perform the following procedure:

1. From the Main Menu, type **2** to select *VLAN Menu*.
2. From the VLAN Menu, type **1** to select *VLAN Definition*.
3. From the VLAN Definition menu, type **2** to select *Modify VLAN*.

The Modify VLAN window in Figure 52 is displayed.

```

Allied Telesyn Ethernet Switch AT-8324 - AT-S25 v2.0.2
Sales
Login Session: Manager                               Module 1 / MASTER

                                Modify VLAN

1 - Select VLAN ID (VID) to modify
S - Save Configuration changes
R - Return to Previous Menu
Enter your selection? _

```

Figure 50 Modifying VLAN Menu

4. Type **1** to select *VLAN ID (VID)*.

The following prompt is displayed:

```
Enter new value -> [1 to 2048] ->
```

5. Enter the VID of the VLAN you want to modify. Press the Enter key.

The Modify VLAN window for the selected VLAN is displayed. This window contains all relevant information about the VLAN.

6. To change a VLAN's name, type **1** to select *VLAN Name* and enter the new name when prompted.

A VLAN must have a name. A VLAN's name must be unique on the stack. You cannot assign the same name to two VLANs in the same stack. A name can be from one to nineteen alphanumeric characters and must contain at least one alphabetic character. It

should reflect the function of the nodes of the VLAN (for example, Sales or Accounting). The name can not contain spaces nor special characters, such as asterisks (*) or exclamation points (!).

7. You are now ready to add or delete ports from the VLAN. But before you do, examine the prompt in the upper right portion of the window to determine the switch module of the stack your management session is currently addressing. If there are ports on this switch you want to add or remove from the VLAN, then continue with the following sub-steps. If this switch does not contain ports that you want to add or remove from the VLAN, then go to the next step to change switches.

To add or remove ports from the VLAN, do the following:

- a. To add or remove tagged ports, type **3** to select *Tagged Ports* and enter the new tagged port list at the prompt. You can specify the ports individually (e.g., 2,5,11), as a range (e.g., 5-10), or both (e.g., 3,7,11-15,17). To specify all ports on the switch, enter ALL. To remove all tagged ports that are assigned to the VLAN from the currently selected switch module, enter NONE.
- b. To add or remove untagged ports, type **4** to select *Untagged Ports* and enter the new untagged port list at the prompt. You can specify the ports individually (e.g., 2,5,11), as a range (e.g., 5-10), or both (e.g., 3,7,11-15,17). To specify all ports on the switch, enter ALL. To remove all untagged ports that are assigned to the VLAN from the currently selected switch module, enter NONE.

Note

You cannot remove untagged ports directly from the Default_VLAN. To remove an untagged port from the Default_VLAN, you must assign it as an untagged port in another VLAN.

- c. If there are ports on other switches in the stack that you want to add or remove from the VLAN, change switch modules by performing Step 8. Otherwise, skip to Step 9.
8. To add or remove ports from a VLAN from different switch modules in a stack, you must change switches by doing the following:
 - a. Type **M** to choose *Select another module*.

The prompt message is displayed:

```
Select Module ID: [1 to 8] ->
```

- b. Enter the ID of the switch module you want to change to, and press the Enter key.
- c. Go to Step 7 and add or remove ports.

9. Type **U** to select *Update VLAN*.

The changes to the VLAN are activated on the stack.

10. Type **S** to select *Save Configuration changes*.

11. Repeat this procedure to modify other VLANs.

Displaying VLAN Information

To view the name, VID number, and member ports of all the VLANs on a switch, perform the following procedure:

1. From the Main Menu, type **2** to select *VLAN Menu*.
2. From the VLAN Menu, type **1** to select *VLAN Definition*.
3. From the VLAN Definition menu, type **4** to select *Show All VLANs*.

The Show All VLANs window is displayed. An example of the window is shown in Figure 51.

```

Allied Telesyn Ethernet Switch AT-8324 - AT-S25 v2.0.2
Sales
Login Session: Manager                               Module 1 / MASTER

Show All VLANs
VID  VLAN Name          VID  VLAN Name
-----
1    Default_VLAN      2    Sales
3    Production
D - Display VLAN Ports
R - Return to Previous Menu
Enter your selection?

```

Figure 51 Show All VLANs Window

Deleting a VLAN

This procedure deletes a port-based or tagged VLAN from a stack.

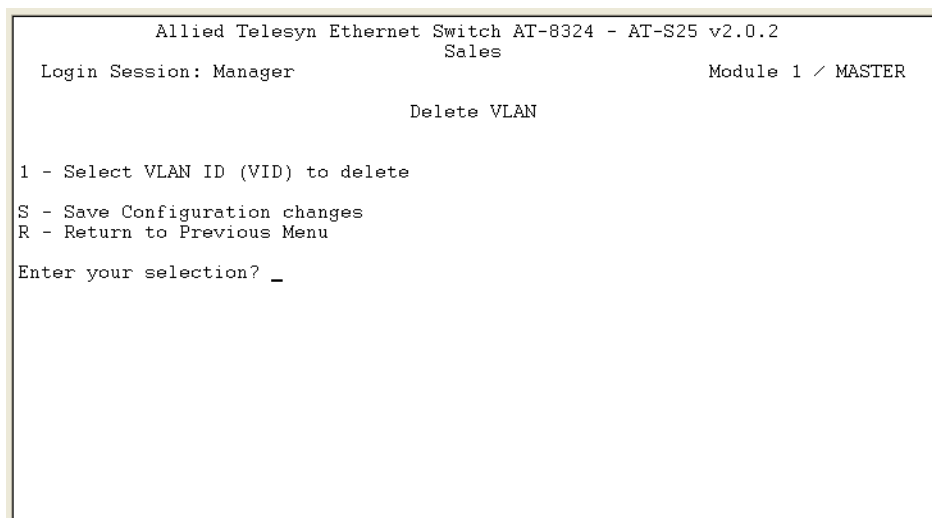
Note

To delete a VLAN, you need to know its VID. To view a VLAN's VID, perform to the procedure **Displaying VLAN Information** on page 137.

To delete a VLAN, perform the following procedure:

1. From the Main Menu, type **2** to select *VLAN Menu*.
2. From the VLAN Menu, type **1** to select *VLAN Definition*.
3. From the VLAN Definition menu, type **3** to select *Delete VLAN*.

The Delete VLAN menu in Figure 52 is displayed.



```

Allied Telesyn Ethernet Switch AT-8324 - AT-S25 v2.0.2
Sales
Login Session: Manager                               Module 1 / MASTER

Delete VLAN

1 - Select VLAN ID (VID) to delete
S - Save Configuration changes
R - Return to Previous Menu
Enter your selection? _

```

Figure 52 Delete VLAN Menu

4. Type **1** to select *Select VLAN ID (VID) to delete*.

The following prompt is displayed:

```
Enter new value -> [2 to 2048] ->
```

5. Enter the VID of the VLAN you want to delete and press the Enter key.

Note

You cannot delete the Default_VLAN, which has a VID of 1.

The specifications of the selected VLAN are displayed. Use this window to confirm that you are deleting the correct VLAN.

6. Type **D** to delete the VLAN or **R** to cancel the procedure.

The following confirmation prompt is displayed:

```
Are you sure you want to delete this VLAN (Y/N)
[Yes/No] ->
```

7. Type **Y** to delete the VLAN or **N** to cancel the procedure. Press the Enter key.

If **Y** is selected, the VLAN is deleted from the stack and the following prompt is displayed:

```
VLAN Delete Operation was successful!
```

```
Please make sure to manually delete any static MAC
address entries for this VLAN
```

All untagged ports in the deleted VLAN are returned to the Default_VLAN as untagged ports.

8. Press any key to continue.
9. Type **S** to select *Save Configuration changes*.
10. Repeat this procedure starting with Step 4 to delete other VLANs.

Deleting All VLANs

This section contains the procedure for deleting all VLANs, except the Default_VLAN, from a stack. To delete selected VLANs, perform the procedure **Deleting a VLAN** on page 138.

To delete all VLANs on a stack, perform the following procedure:

1. From the Main Menu, type **2** to select *VLAN Menu*.
2. From the VLAN Menu, type **1** to select *VLAN Definition*.
3. From the VLAN Definition menu, type **6** to select *Clear All VLANs*.

A following confirmation message is displayed:

```
This operation deletes ALL user created VLANs!  
Do you want to continue [Yes/No] ->
```

4. Type **Y** to delete all VLANs or **N** to cancel the procedure. Press the Enter key.

Another confirmation message is displayed:

```
Clear All VLANs Operation was successful!
```

```
Please make sure to manually update any static MAC  
address entries Press any key to continue...
```

All VLANs are deleted and their tagged and untagged ports are returned to the Default_VLAN as untagged ports.

5. Press any key to continue.
6. Type **S** to select *Save Configuration changes*.

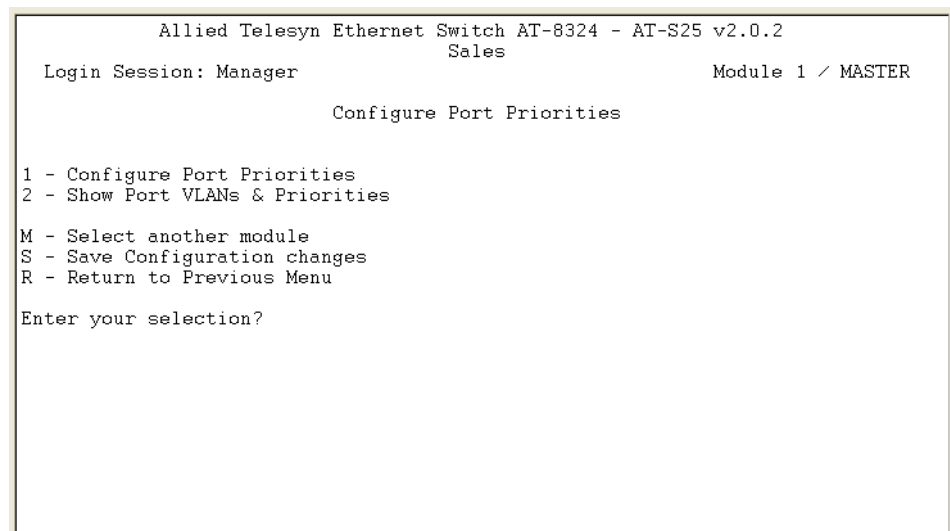
Displaying PVIDs

The following procedure displays a window that lists the PVIDs for all the ports on the switch. You cannot change the PVID of a port. The AT-S25 management software automatically sets the PVID when a port is made an untagged member of a VLAN, assigning it a PVID value equal to the VID.

The window described in this section also contains the priority queue settings for each port. To display the PVID settings on the switch, perform the following procedure:

1. From the Main Menu, type **2** to select *VLAN Menu*.
2. From the VLAN Menu, type **2** to select *Configure Port Priorities*.

The Configure Port Priorities menu in Figure 54 is displayed.



```

Allied Telesyn Ethernet Switch AT-8324 - AT-S25 v2.0.2
Sales
Login Session: Manager                               Module 1 / MASTER

Configure Port Priorities

1 - Configure Port Priorities
2 - Show Port VLANs & Priorities

M - Select another module
S - Save Configuration changes
R - Return to Previous Menu

Enter your selection?
  
```

Figure 53 Configure Port Priorities Menu

3. If necessary, use the **M - Select another module** option to change to another switch module in the stack.
4. From the Configure Port Priorities window, type **2** to select *Show Port VLANs & Priorities*.

The Show Port VLANs & Priorities window is displayed. An example of the window is shown in Figure 54 on page 142.

Allied Telesyn Ethernet Switch AT-8324 - AT-S25 v2.0.2
Sales
Login Session: ManagerModule 1 / MASTER

Show Port VLANs & Priorities

Port	PVID	Priority	Override Priority
01	1	0	No
02	1	0	No
03	1	0	No
04	1	0	No
05	1	0	No
06	1	0	No
07	1	0	No
08	1	0	No

N - Next Page
M - Select another module
R - Return to Previous Menu
Enter your selection? _

Figure 54 Show Port VLANs and Priorities Window

The PVID column displays the current PVID value for each switch port.

Note
The Priority and Override Priority columns relate to the switch’s Class of Service feature. For information, refer to **Chapter 11, Class of Service** on page 161.

Specifying a Management VLAN

In order for you to remotely manage an AT-8316F or AT-8324 Switch, there must exist a communications path through which the management station and the switch to be managed can communicate. If the management station is connected directly to a port on the switch, either through a tagged or untagged port, then the communications path automatically exists and you could fully manage the switch.

However, if there is one or more intermediate Ethernet switches between the management station and the switch to be managed, then it may be necessary for you to manually create a communications path. This is accomplished by specifying a management VLAN.

The management VLAN is the VLAN through which a remote management station communicates with a managed switch. By default, the management VLAN is the Default_VLAN. If you do not create any new VLANs in your network and if your AT-8316F and AT-8324 Switches are interconnected with either tagged or untagged ports, then you will not need to create or specify a new management VLAN.

However, if you do create additional VLANs in your network, then you might need to change a management VLAN. Below are several rules to observe when using this feature:

- ☐ The management VLAN must exist on each AT-8316F or AT-8324 Switch that you wish to manage.
- ☐ The uplink and downlink ports on each switch that are functioning as the tagged or untagged data links between the switches must be either tagged or untagged members of the management VLAN.
- ☐ The port on the switch to which the management station is connected must be a member of the management VLAN. (This rule does not apply when managing the switch locally through the RS-232 Terminal Port.)

Here is an example. Let's assume that you have a stack of seven AT-8316F and/or AT-8324 Switches with one Master switch. If the uplink and downlink ports between the various switches are members of the Default_VLAN and if the management station is connected to a port of the Default_VLAN, you will be able to manage all the switches since the Default_VLAN is by default the management VLAN.

Now let's assume that you have decided to create a VLAN called NMS with a VID of 24 for the sole purpose of remote network management. For this, you would need to create the NMS VLAN on each AT-8316F or AT-8324 Switch that you wish to manage remotely, being sure to assign each NMS VLAN the VID of 24. You would also need to specify the NMS VLAN as the management VLAN on each switch using the management software. Finally, you would need to connect your management station to a port on a switch that is a tagged or untagged member of the management VLAN.

To specify the management VLAN in the AT-S25 software, perform the following procedure:

1. From the Main Menu, type **2** to select *VLAN Menu*.
2. From the VLAN Menu, type **3** to select *Management VLAN*.

The following prompt is displayed:

```
Enter Management VLAN ID [1 to 2048] ->
```

3. Specify the VID of the VLAN that is to function as the management VLAN. This VLAN must already exist on the switch. Press the Enter key.

The following prompt is displayed:

```
SUCCESS - Press any key to continue ...
```

4. Press any key to continue.
5. Type **S** to select *Save Configuration changes*.

Switching the VLAN Mode

To switch a VLAN's mode from Tagged to Basic, or vice versa, perform the following procedure:

1. From the Main Menu, type **5** to select *System Config Menu*.

The System Config Menu in Figure 47 is displayed.

```

Allied Telesyn Ethernet Switch AT-8324 - AT-S25 v2.0.2
Sales
Login Session: Manager                               Module 1 / MASTER

System Config Menu

1 - Switch Mode ..... Tagged
2 - Console Disconnect Timer Interval ... 10 minute(s)
3 - SNMP Access ..... Disabled
4 - Web Server Status..... Enabled
5 - MAC address aging time ..... 300 second(s)
6 - Reset Configuration to Factory Defaults

A - Advanced Configuration
S - Save Configuration changes
R - Return to Previous Menu

Enter your selection? _

```

Figure 55 System Config Menu

2. Type **1** to select *Switch Mode* and press the Enter key.

The prompt message is displayed:

The switch will be rebooted after changing the switch mode.

Do you want to continue? (Y/N):

3. Type **Y** to accept the change, or type **N** to cancel.

Chapter 10

MAC Address Table

The chapter contains the procedures for viewing the static and dynamic MAC addresses in the MAC address table. The sections in this chapter include:

- ☐ **MAC Address Overview** on page 147
- ☐ **Viewing MAC Addresses** on page 149
- ☐ **Viewing MAC Addresses by Port & Module** on page 154
- ☐ **Viewing the MAC Addresses of a VLAN** on page 155
- ☐ **Identifying a Port or a Module Number by MAC Address** on page 156
- ☐ **Deleting MAC Addresses** on page 157
- ☐ **Deleting All Dynamic MAC Addresses** on page 158
- ☐ **Adding Static and Multicast MAC Addresses** on page 159
- ☐ **Changing the Aging Time** on page 160

MAC Address Overview

The AT-8300 Series switch has a MAC address table up to 12K in size. The switch uses the table to store the MAC addresses of the network nodes connected to its ports, along with the port number on which each address was learned.

The devices that you connect to your network have a unique MAC address. A MAC address is assigned to a device by the device's manufacturer. For example, every network interface card that you use to connect your computers to your network has a MAC address assigned to it by the adapter's manufacturer.

The switch learns the MAC addresses of the end nodes by examining the source address of each packet received on a port. It adds the address and port on which the packet was received to the MAC table if the address has not already been entered in the table. The result is a table that contains all the MAC addresses of the devices that are connected to the switch's ports, and the port number where each address was learned.

When a switch receives a packet, it also examines the destination address and, by referring to its MAC Address Table, determines the port where the destination node is connected. It then forwards the packet to the appropriate port and on to the end node. This increases network bandwidth by limiting each frame to the appropriate port when the intended end node is located, freeing the other switch ports for receiving and transmitting data.

If the switch receives a packet with a destination address that is not in the MAC Address Table, it floods the packet to all the ports on the switch. If the ports have been grouped into virtual LANs, the switch floods the packet only to those ports which belong to the same VLAN as the port on which the packet was received. This prevents packets from being forwarded onto inappropriate LAN segments and increases network security. When the destination node responds, the switch adds its MAC address and port number to the table.

If the switch receives a packet with a destination address that is on the same port on which the packet was received, it discards the packet without forwarding it on to any port. Since both the source node and the destination node for the packet are located on the same port on the switch, there is no reason for the switch to forward the packet. This too increases network performance by preventing frames from being forwarded unnecessarily to other network devices.

The type of MAC address described above is referred to as a *dynamic MAC address*. Dynamic MAC addresses are addresses that the switch learns by examining the source MAC addresses of the frames received on the ports.

Dynamic MAC addresses are not stored indefinitely in the MAC Menu. The switch deletes a dynamic MAC address from the table if it does not receive any frames from the node after a specified period of time. The switch assumes that the node with that MAC address is no longer active and that its MAC address can be purged from the table. This prevents the MAC Address Table from becoming filled with addresses of nodes that are no longer active.

The period of time that the switch waits before purging an inactive dynamic MAC address is called the *MAC aging time*. This value is adjustable on the AT-8316F or AT-8324 Switch. The default value is 300 seconds (5 minutes). For instructions on changing the aging timer, refer to **Changing the Aging Time** on page 160.

The MAC Address Table can also store *static MAC addresses*. A static MAC address, once entered in the table, remains in the table indefinitely and is never deleted, even when the end node is inactive.

You might need to enter static MAC addresses of end nodes the switch will not learn in its normal dynamic learning process, or if you wish a MAC address to remain permanently in the table, even when the end node is inactive.

Note

Due to chip set constraints, a port link state that changes from 'up' to 'down' will cause the addresses learned for that port group⁽¹⁾ to be flushed.

⁽¹⁾ A port group is considered one of the following:
Ports 1-8, ports 9-16, ports 17-24, ports A(x), ports B(x), where A and B are the option module slots.

Viewing MAC Addresses

To display the MAC Menu, perform the following procedure:

1. From the Main Menu, type **6** to select *MAC Menu*.

The MAC Menu in Figure 56 is displayed.

```

Allied Telesyn Ethernet Switch AT-8324 - AT-S25 v2.0.2
Sales
Login Session: Manager                               Module 1 / MASTER

MAC Menu

1 - Show all MAC addresses
2 - Show all static MAC addresses
3 - Show all multicast MAC addresses
4 - Show MAC addresses on base ports
5 - Show MAC addresses by module
6 - Show MAC addresses by VLAN ID
7 - Show MAC addresses by port & module
8 - Show port and module number of MAC address
9 - Add static MAC Address
A - Delete MAC Address
B - Delete all dynamic MAC addresses

S - Save Configuration changes
R - Return to Previous Menu

Enter your selection? _

```

Figure 56 MAC Menu

Viewing All MAC Addresses

To display all the MAC addresses, including the static, dynamic, or multicast MAC addresses, perform the following procedure:

1. From the Main Menu, type **6** to select *MAC Menu*.
2. From the MAC Menu, type **1** to select *Show all MAC addresses*.

A window is displayed with all the MAC addresses learned by the stack. An example of the Show all MAC addresses window is displayed, as shown in Figure 57.

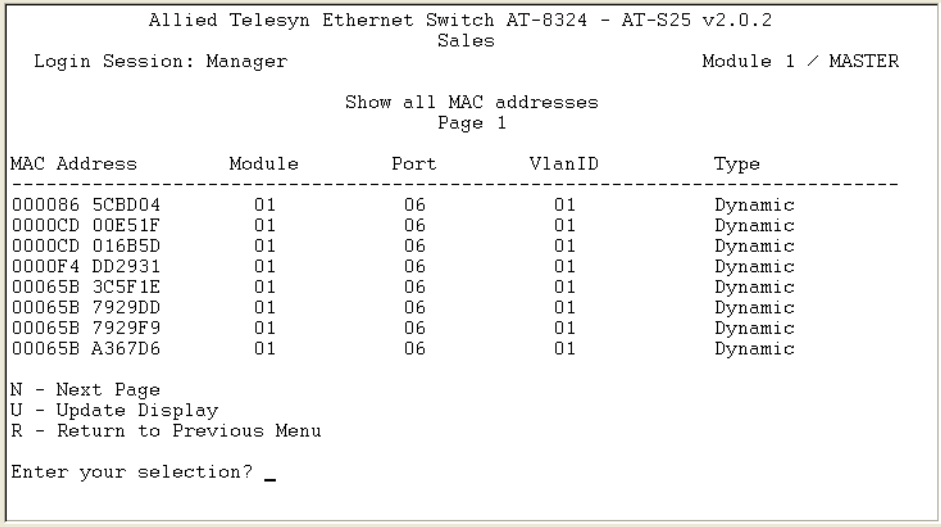


Figure 57 Show all MAC addresses Window

Table 11 lists the parameters appeared in the Show all MAC addresses window. These parameters are for viewing purposes only.

Table 11 Show all MAC address Parameters

PARAMETER	DESCRIPTION
MAC Address	The MAC address of the node connected to the port.
Module	The switch module in the stack where the MAC address was learned.
Port	The port on the switch where the MAC address was learned.
VlanID	The VID of the VLAN where the port is an untagged member.
Type	The MAC address type. The type can be either static, dynamic, or multicast.

Viewing Static MAC Addresses Only

To display only static MAC addresses, perform the following procedure:

1. From the Main Menu, type **6** to select *MAC Menu*.
2. From the MAC Menu, type **2** to select *Show all static MAC addresses*.

A window is displayed with all the MAC addresses. An example of the Show all MAC addresses window is displayed in Figure 58.

```

Allied Telesyn Ethernet Switch AT-8324 - AT-S25 v2.0.2
Sales
Login Session: Manager
Module 1 / MASTER

Show all static MAC addresses
Page 1

MAC Address      Module      Port      VlanID      Type
-----
00A0D2 978F3E    01         00         01         Static

U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 58 Show all static MAC addresses Window

This window is exactly the same as the Show all static MAC address window, except for the title and the fact that it displays only static MAC addresses. For information displayed in this window, refer to the Table 11 in **Viewing All MAC Addresses** on page 149.

Note

The MAC address of Module 1/Master switch will always be displayed as a static MAC address on Port 00.

**Viewing
Multicast MAC
Addresses Only**

- To display only multicast MAC addresses, perform the following procedure:
1. From the Main Menu, type **6** to select MAC Menu.
 2. From the MAC Menu, type **3** to select *Show all multicast MAC addresses*.
- A window is displayed with all the multicast MAC addresses. An example of the Show all multicast MAC addresses window is shown in Figure 59.

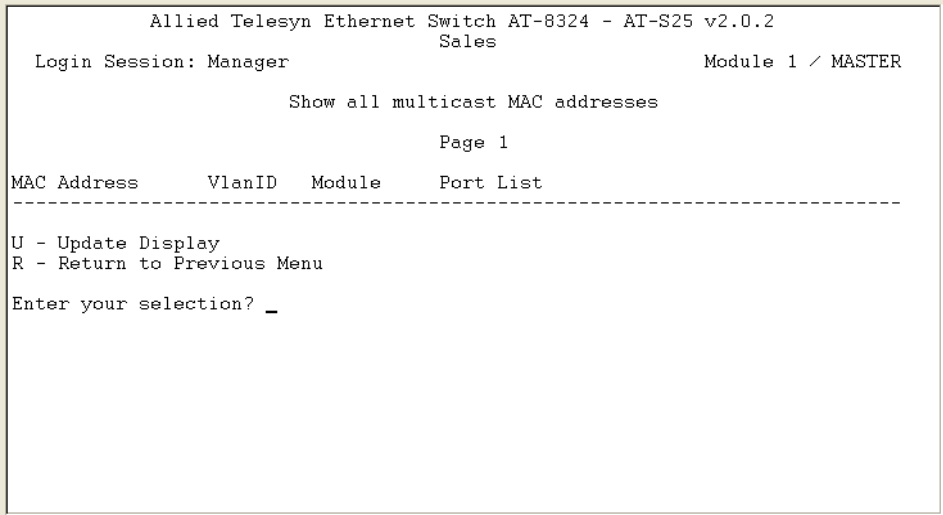


Figure 59 Show all multicast MAC addresses Window

Table 12 lists the parameters used in the Show all multicast MAC addresses window.

Table 12 Show all multicast MAC addresses Parameters

PARAMETER	DESCRIPTION
MAC Address	The multicast MAC address.
VlanID	The VID of the VLAN where the port is an untagged member.
Module	The selected module.
Port List	The port list on the switch where the multicast MAC address was learned.

Viewing MAC Addresses on Base Ports Only

This selection is useful if you are managing an AT-8300 Series stack that has switches containing optional expansion modules. You could use this selection to view only those MAC addresses learned on the base ports of the switches and exclude the ports on the expansion modules.

To view only the MAC addresses learned on the base ports, perform the following procedure:

1. From the Main Menu, type **6** to select *MAC Menu*.
2. From the MAC Menu, type **4** to select *Show MAC addresses on base ports*.

A window is displayed with the MAC addresses on the base ports. An example of the Show MAC addresses on base ports window is shown in Figure 60.

```

Allied Telesyn Ethernet Switch AT-8324 - AT-S25 v2.0.2
Sales
Login Session: Manager
Module 1 / MASTER

Show MAC addresses on base ports
Page 1

MAC Address      Module    Port    VlanID    Type
-----
000086 5CBD04    01       06       01       Dynamic
0000CD 00E51F    01       06       01       Dynamic
0000CD 016B5D    01       06       01       Dynamic
0000F4 DD2931    01       06       01       Dynamic
000272 002262    01       06       01       Dynamic
00065B 230F7E    01       06       01       Dynamic
00065B 3C5F1E    01       06       01       Dynamic
00065B 7929DD    01       06       01       Dynamic

N - Next Page
U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 60 Show MAC addresses on base ports Window

This window is exactly the same as the Show all MAC addresses window, except for the title. For information displayed in this window, refer to the Table 11 in **Viewing All MAC Addresses** on page 149.

Viewing MAC Addresses by Port & Module

This section contains the procedure for viewing the dynamic MAC addresses that have been learned on a particular port. You could also use this procedure to view any static MAC addresses that have been assigned to a port.

1. From the Main Menu, type **6** to select *MAC Menu*.
2. From the MAC Menu, type **7** to select *Show MAC addresses by port & module*.

The following prompt is displayed:

```
Please enter module number -> [1 to 8] ->
```

3. Enter the number of the module whose static and dynamic MAC addresses you wish to view and press the Enter key.

The following prompt is displayed:

```
Please enter port number -> [1 - 24] ->
```

4. Enter the number of the port whose static and dynamic MAC addresses you wish to view and press the Enter key.

A window is displayed with the MAC addresses of the end nodes on the port. For information displayed in this window, refer to the Table 11 in **Viewing All MAC Addresses** on page 149.

The information in this window is for viewing purposes only.

Viewing the MAC Addresses of a VLAN

The procedure in this section can be useful if you created VLANs on the switch and want to view the MAC addresses of the nodes of a particular VLAN. (This procedure is not of much value if the switch contains only the Default VLAN, in which case displaying the entire MAC address table, as explained earlier in this chapter, produces the same result.)

Note

To perform this procedure, you need to know the VID number of the VLAN whose MAC addresses you want to view. To obtain a VLAN's VID, refer to **Displaying VLAN Information** on page 137.

To view the MAC addresses of a VLAN on the switch, perform the following procedure.

1. From the Main Menu, type **6** to select *MAC Menu*.
2. From the MAC Menu, type **6** to select *Show MAC addresses by VLAN ID*.

The following prompt is displayed:

```
Please enter a VLAN ID: [1 to 2048] ->
```

3. Enter the VID of the desired VLAN and press the Enter key.

The management software displays a window with a list of the MAC addresses of the nodes in the VLAN. For information displayed in this window, refer to the Table 11 in **Viewing All MAC Addresses** on page 149.

Identifying a Port or a Module Number by MAC Address

In some situations, you might want to know which port a particular MAC address was learned. You could display the MAC Menu and scroll through the list looking for the MAC address. But if the switch is part of a large network, finding the address could prove difficult.

The procedure in this section offers an easier way. You could specify the MAC address and let the management software automatically locate the port on the switch where the device is connected.

1. From the Main Menu, type **6** to select *MAC Menu*.
2. From the MAC Menu menu, type **8** to select *Show port and module number of MAC address*.

The following prompt is displayed:

```
Please enter MAC address:
```

3. Enter the MAC address of the node in the following format and press the Enter key:

```
XXXXXX XXXXXX
```

The following prompt is displayed:

```
Please enter VLAN ID -> [1 to 2048]:
```

4. Enter the VLAN ID. If no VLAN ID is entered, the default value of "1" will be taken.

The management software displays a prompt containing the port, VLAN Name, and the module number on the switch to which the node is connected, if the address was learned dynamically, or to which the address was assigned, for a static address.

Deleting MAC Addresses

The following procedure explains how to delete a static, dynamic, or multicast MAC address from the MAC Menu.

To delete an address from the MAC Menu, perform the following procedure:

1. From the Main Menu, type **6** to select *MAC Menu*.
2. From the MAC Menu, type **A** to select *Delete MAC Address*.

The following prompt is displayed:

```
Please enter a MAC address ->
```

3. Enter the MAC address to be deleted in the following format and press the Enter key:

```
XXXXXX XXXXXX
```

The following prompt is displayed:

```
Please enter VLAN ID -> [1 to 2048] ->
```

4. Enter the VID of the desired VLAN and press the Enter key.

The MAC address is deleted from the switch's MAC Address Table.

Note

You could not delete a switch's MAC address, an STP BPDU MAC address, or a broadcast address.

5. Repeat the procedure to delete additional MAC addresses.

Deleting All Dynamic MAC Addresses

The management software allows you to purge the MAC Menu of all dynamic MAC addresses. Once the table has been purged, the switch immediately begins to relearn the MAC addresses as frames are received on the ports.

Note

This procedure does not delete static MAC addresses.

To delete all dynamic MAC addresses from the MAC Menu, perform the following procedure.

1. From the Main Menu, type **6** to select *MAC Menu*.
2. From the MAC Menu menu, type **B** to select *Delete all dynamic MAC addresses*.

A following prompt is displayed:

```
All dynamic MAC addresses will be deleted.
```

```
Do you want to continue? [Yes/No] ->
```

3. Type **Y** for Yes to delete the dynamic MAC addresses or **N** for No to cancel the procedure.

If you type **Y** for Yes, the dynamic MAC addresses are deleted from the MAC Address Table. The switch immediately begins to relearn the addresses and to add them to the table.

Adding Static and Multicast MAC Addresses

This section contains the procedure for adding the static and multicast addresses to the switch. You could assign up to 150 static MAC addresses on a stack of an AT-8316F or an AT-8324 Switch.

To add a static or multicast address to the MAC Menu, perform the following procedure:

1. From the Main Menu, type **6** to select *MAC Menu*.
2. From the MAC Menu, type **9** to select *Add static MAC address*.

The following prompt is displayed:

```
Please enter MAC address ->
```

3. Enter the static MAC address in the following format:

```
XXXXXX XXXXXX
```

Once you have specified the MAC address, the following prompts are displayed:

```
Please enter VLAN ID -> [1 to 2048] ->
```

4. Enter the VID of the desired VLAN and press the Enter key.

```
Please enter a port number: [1 to 24] ->
```

5. Enter the number of the port on the switch to which you wish to assign the address.

The management software adds the address to the MAC Menu.

6. Repeat steps 2 to 4 to enter additional static or multicast MAC addresses.

Changing the Aging Time

The switch uses the aging time to delete inactive dynamic MAC addresses from the MAC Menu. When the switch detects that no packets have been sent to or received from a particular MAC address in the table after the period specified by the aging time, the switch deletes the address. This prevents the table from becoming full of addresses of nodes that are no longer active.

To adjust the aging time, perform the following procedure:

1. From the Main Menu, type **5** to select *System Config Menu*.
2. From the *System Config Menu*, type **5** to select *MAC address aging time*.

The following prompt is displayed:

```
Enter MAC address aging time -> [8 to 512]
```

3. Enter a new value in seconds. The range of the MAC Address aging time is 8 to 512 seconds. The default value is 300 seconds (5 minutes).

Changes to the settings take effect immediately on the switch.

Chapter 11

Class of Service

This chapter contains the procedures for configuring the Class of Service (CoS) feature of the AT-S25 software. Sections in the chapter include:

- ❑ **Class of Service Overview** on page 162
- ❑ **Configuring CoS** on page 163
- ❑ **Show Port VLANs & Priorities** on page 165

Class of Service Overview

The AT-8316F or AT-8324 Switch supports CoS as specified in the IEEE 802.1p and 802.1Q standards. CoS can be important in network environments where there are time-critical applications, such as voice transmission or video conferencing, that can be adversely affected by packet transfer delays.

Prior to CoS, network traffic was handled in a best-effort manner. File transfer delays did occur, but were mostly transparent to network users. But with the introduction of time-critical applications, packet transfer delays can prove problematic. For example, transfer delays of voice transmission can result in poor audio quality.

CoS was designed to address this problem. The 802.1p standard outlines eight levels of priority, 0 to 7, with 0 the lowest priority and 7 the highest.

The AT-8316F or AT-8324 Switch has two priority queues, low and high. When a priority tagged packet enters a switch port, the switch responds by placing the packet into one of the two queues according to following behaviors:

- ☐ For all IGMP and BPDU packets that are destined to the CPU, the switch sends these packets to “high” queue.
- ☐ For all incoming unicast packets that have unknown destination on the port, the switch sends these packets to “low” queue.
- ☐ For all other port incoming packets, the switch responds as follow.

Note

These priority-to-queue assignments can be overridden using the AT-S25 management software on a per port basis.

Override	Port Priority Level	Tag Priority Level	Priority Queue ¹
-	1	-	high
yes	0	-	low
no	0	> 3	high
no	0	< 4 (or untagged)	low

1. To send a packet to the low queue, one of the following conditions must exist:

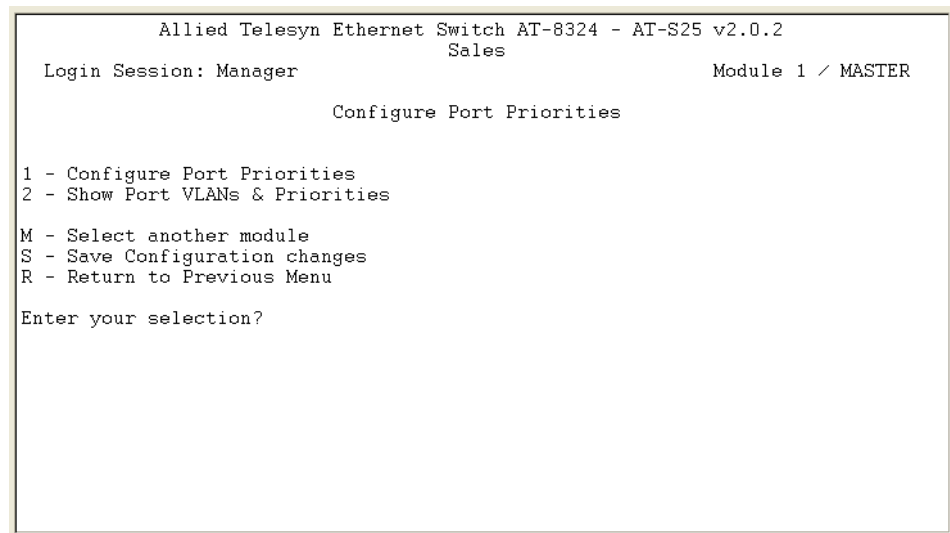
- * Receive a packet with an unknown destination address.
- * Set the override to “yes” and the port priority to “0”.
- * Set the override to “no”, the port priority to “0”, and receive an “untagged” packet or a packet with a priority tag “less than 4”.

Configuring CoS

To configure CoS for a port, perform the following procedure:

1. From the Main Menu, type **2** to select *VLAN Menu*.
2. From the VLAN Menu, type **2** to select *Configure Port Priorities*.

The Configure Port Priorities menu in Figure 61 is displayed.



```

Allied Telesyn Ethernet Switch AT-8324 - AT-S25 v2.0.2
Sales
Login Session: Manager                               Module 1 / MASTER

Configure Port Priorities

1 - Configure Port Priorities
2 - Show Port VLANs & Priorities

M - Select another module
S - Save Configuration changes
R - Return to Previous Menu

Enter your selection?
  
```

Figure 61 Configure Port Priorities Menu

3. Type **1** to select *Configure Port Priorities*.

The following prompt is displayed:

```
Enter port number ->
```

4. Enter the number of the port on the switch where you wish to configure CoS.
5. Press the Enter key. The Configure Port Priorities window in Figure 53 on page 141 is displayed.
6. Type **3** to select *Priority (0-1) 0=Low 1=High*.

The following prompt is displayed:

```
Enter new value -> [0 to 1]
```

7. Type **4** to select *Override Priority*.

The default setting is No. Observe the following when setting the Override Priority.

- ☐ When the Override is set to **No** and the Port Priority Level is set to **0**, all incoming packets are directed to the queue indicated in the Tag Priority Level.
- ☐ When the Override is set to **No** and the Port Priority Level is set to **1**, all incoming packets are directed to “high” priority queue.
- ☐ When the Override is set to **Yes** and the Port Priority Level is set to **0**, all incoming packets are directed to “low” priority queue.

For more information on the assignment of the priority queue, refer to **Class of Service Overview** on page 162.

Note

The tagged information in a frame is not changed as the frame traverses the switch. A tagged frame leaves a switch with the same priority level that it had when it entered, regardless of the priority queue that handled the frame.

8. Type **C** to select *Configure Port Priorities*.
9. Type **S** to select *Save Configuration changes*.

Show Port VLANs & Priorities

To display the port VLANs and priorities, perform the following procedure:

1. From the Main Menu, type **2** to select *VLAN Menu*.
2. From the VLAN Menu, type **2** to select *Configure Port Priorities*.
The Configure Port Priorities menu in Figure 61 on page 163 is displayed.
3. If necessary, use the **M - Select another module** option to change to another switch module in the stack.
4. From the Configure Port Priorities window, type **2** to select *Show Port VLANs & Priorities*.

The Show Port VLANs & Priorities window is displayed. An example of the window is shown in Figure 62.

```

Allied Telesyn Ethernet Switch AT-8324 - AT-S25 v2.0.2
Sales
Login Session: Manager
Module 1 / MASTER

Show Port VLANs & Priorities

Port      PVID      Priority      Override Priority
-----
01         1         0             No
02         1         0             No
03         1         0             No
04         1         0             No
05         1         0             No
06         1         0             No
07         1         0             No
08         1         0             No

N - Next Page
M - Select another module
R - Return to Previous Menu

Enter your selection? _

```

Figure 62 Show Port VLANs & Priorities Window

The PVID column displays the current PVID value for each switch port.

Chapter 12

IGMP Snooping

This chapter explains how to activate and configure the Internet Group Management Protocol (IGMP) snooping feature on the stack. Sections in the chapter include:

- ❑ **IGMP Snooping Overview** on page 167
- ❑ **Activating IGMP Snooping** on page 169
- ❑ **Displaying a List of Host Nodes** on page 172
- ❑ **Displaying a List of Multicast Routers** on page 173

IGMP Snooping Overview

IGMP enables routers to create lists of nodes that are members of multicast groups. (A multicast group is a group of end nodes that want to receive multicast packets from a multicast application.) A router creates a multicast membership list by periodically sending out queries to the local area networks connected to its ports.

A node wanting to become a member of a particular multicast group responds to a query by sending a *report*. A report indicates an end node's intention to become a member of a multicast group. Nodes that join a multicast group are referred to as *host nodes*. Once a host node has been made a member of a multicast group, it must periodically issue reports to remain a member.

Once the router has received a report from a host node, it notes the multicast group that the host node wants to join and the port on the router where the node is located. Any multicast packets belonging to that multicast group are then forwarded by the router out the port. If a particular port on the router has no nodes that want to be members of multicast groups, the router does not send multicast packets out the port. This improves network performance by restricting multicast packets only to router ports where host nodes are located.

There are two versions of IGMP, referred to as Version 1 and Version 2. One of the differences between the two versions is how a host node indicates that it no longer wants to be a member of a multicast group.

In Version 1, it simply stops sending reports. If a router does not receive a report from a host node after a predefined length of time, referred to as a *time-out value*, it assumes that the host node no longer wants to receive multicast frames, and removes it from the membership list of the multicast group.

In Version 2, a host node exits from a multicast group by sending a *leave request*. Once a router receives a leave request from a host node, it removes the node from appropriate membership list. The router will also stop sending out multicast packets out the port to which the node is connected if it determines there are no further host nodes on the port.

IGMP snooping enables the Fast Ethernet switch to monitor the flow of queries from a router and reports from host nodes to build its own multicast membership lists. It uses the lists to forward multicast packets only to switch ports where there are host nodes that are members of multicast groups. This improves switch performance and network security by restricting the flow of multicast packets only to those switch ports connected to host nodes.

Without IGMP snooping, a switch would have to flood multicast packets out all of its ports, except the port on which it received the packet. Such flooding of packets can negatively impact the switch and network performance.

The AT-8300 Series switch supports both IGMP Version 1 and Version 2. The switch maintains its multicast groups through an adjustable time-out value, which controls how frequently it expects to see reports from end nodes that want to remain members of multicast groups, and by processing leave requests.

Note

By default, IGMP snooping is disabled on the switch.

Activating IGMP Snooping

To activate or deactivate IGMP snooping on the stack and to configure IGMP snooping parameters, perform the following procedure:

1. From the Main Menu, type **5** to select *System Config Menu*.
2. From the System Config Menu, type **A** to select *Advanced Configuration*.
3. From the Advanced Configuration window, type **1** to select *IGMP Snooping Configuration*.

The IGMP Snooping Configuration menu in Figure 63 is displayed.

```

Allied Telesyn Ethernet Switch AT-8324 - AT-S25 v2.0.2
Sales
Login Session: Manager                               Module 1 / MASTER

IGMP Snooping Configuration

1 - IGMP Snooping Status ..... Disabled
2 - Multicast Host Topology ..... Single-Host/Port (Edge)
3 - Host/Router Timeout Interval ..... 260 seconds
4 - Maximum Multicast Groups ..... 256
5 - View Multicast Hosts List
6 - View Multicast Routers List

S - Save Configuration changes
R - Return to Previous Menu

Enter your selection? _

```

Figure 63 IGMP Snooping Configuration Menu

Table 13 lists the parameters appeared in the IGMP Snooping Configuration menu.

Table 13 IGMP Snooping Configuration Parameters

PARAMETER	DESCRIPTION
1 - IGMP Snooping Status	Enables and disables IGMP snooping on the stack. After selecting this option, type E to enable or D to disable this feature.
2 - Multicast Host Topology	<p>Defines whether there is only one host node per stack port or multiple host nodes per port.</p> <p>Possible settings for this parameter are:</p> <ul style="list-style-type: none"> • Single-Host/Port (Edge): This setting is appropriate when there is only one host node connected to each port on the stack. This setting causes the stack to immediately stop sending multicast packets out a stack port when a host node signals its desire to leave a multicast group by sending a leave request or when the host node stops sending reports. The stack responds by immediately ceasing the transmission of further multicast packets out the port where the host node is connected. • Multi-Host/Port (Intermediate): This setting is appropriate if there is more than one host node connected to a stack port, such as when a port is connected to an Ethernet hub to which multiple host nodes are connected. With this setting selected the stack continues sending multicast packets out a port even after it receives a leave request from a host node on the port. This ensures that the remaining active host nodes on the port will continue to receive the multicast packets. Only after all the host nodes connected to a stack port have transmitted leave requests (or have timed out) will the stack stop sending multicast packets out the port. <p>If a stack has a mixture of host nodes, that is, some connected directly to the stack and others through an Ethernet hub, you should select the <i>Multi-Host Port</i> selection.</p>

PARAMETER	DESCRIPTION
3 - Host/Router Timeout Interval	<p>Specifies the time period in seconds after which the stack determines that a host node has become inactive. An inactive host node is a node that has not sent an IGMP report during the specified time interval. The range is from 1 second to 86,400 seconds (24 hours). The default is 260 seconds.</p> <p>This parameter also specifies the time interval used by the stack in determining whether a multicast router is still active. The stack makes the determination by watching for queries from the router. If the stack does not detect any queries from a multicast router during the specified time interval, it assumes that the router is no longer active on the port.</p>
4 - Maximum Multicast Groups	<p>Specifies the maximum number of multicast groups the stack will learn. The range is 1 to 255 groups. The default is 64 multicast groups.</p> <p>This parameter is useful with networks that contain a large number of multicast groups. You could use the parameter to prevent the stack's MAC Address Table from filling up with multicast MAC addresses, leaving no room for dynamic or static MAC addresses.</p>

Note

Selections 5 and 6 in the menu are discussed later in this chapter.

- After making the desired changes, type **S** to select *Save Configuration changes*.

Changes to the parameters take effect immediately on the stack.

Displaying a List of Host Nodes

You could use the AT-S25 software to display a list of the multicast groups on a stack, as well as the host nodes. To display the list, perform the following procedure:

1. From the Main Menu, type **5** to select *System Config Menu*.
2. From the System Config Menu, type **A** to select *Advanced Configuration*.
3. From the Advanced Configuration window, type **1** to select *IGMP Snooping Configuration*.

The IGMP Snooping Configuration window in Figure 63 is displayed.

4. From the IGMP Snooping Configuration window, type **5** to select *View Multicast Hosts List*.

The View Multicast Hosts List in Figure 64 is displayed.

```

Allied Telesyn Ethernet Switch AT-8324 - AT-S25 v2.0.2
Sales
Login Session: Manager                               Module 1 / MASTER

View Multicast Hosts List

=====
MulticastGroup      VLAN      Module  Port      HostIP
=====
U - Update Display
R - Return to Previous Menu
Enter your selection? _

```

Figure 64 View Multicast Hosts List Window

Table 14 lists the parameters appeared in the View Multicast Hosts List window. These parameters are for viewing purposes only.

Table 14 View Multicast Hosts List Parameters

PARAMETER	DESCRIPTION
MulticastGroup	The multicast address of the group.
VLAN	The VID of the VLAN in which the port is an untagged member.
Module	The module on the stack that is being used.
Port	The port(s) on the stack to which one or more host nodes of the multicast group are connected.
Host IP	The IP address(es) of the host node(s) connected to the port.

Displaying a List of Multicast Routers

A multicast router is a router that is receiving multicast packets from a multicast application and transmitting the packets to host nodes. You could use the AT-S25 software to display a list of the multicast routers that are connected to the stack.

To display a list of the multicast routers, perform the following procedure:

1. From the Main Menu, type **5** to select *System Config Menu*.
2. From the System Config Menu, type **A** to select *Advanced Configuration*.
3. From the Advanced Configuration window, type **1** to select *IGMP Snooping Configuration*.
4. From the IGMP Snooping Configuration window, type **6** to select *View Multicast Routers List*.

The View Multicast Router List window in Figure 64 is displayed.

```

Allied Telesyn Ethernet Switch AT-8324 - AT-S25 v2.0.2
Sales
Login Session: Manager                               Module 1 / MASTER

View Multicast Routers List

=====
Module      Port      VLAN      RouterIP
=====
U - Update Display
R - Return to Previous Menu
Enter your selection? _

```

Figure 65 View Multicast Routers List Window

Table 15 lists the parameters appeared in the View Multicast Routers List window. These parameters are for viewing purposes only.

Table 15 View Multicast Routers List Parameters

PARAMETER	DESCRIPTION
Module	The module on the stack that is being used.
Port	The port on the stack where the multicast router is connected.
VLAN	The VID of the VLAN in which the port is an untagged member.
RouterIP	The IP address of the multicast router.

Chapter 13

Ethernet Statistics

This chapter contains the procedures for displaying and clearing data traffic statistics. Sections in the chapter include:

- ❑ **Displaying Port Statistics** on page 175
- ❑ **Displaying Switch Statistics** on page 177

Displaying Port Statistics

To display Ethernet port statistics, perform the following procedure:

1. From the Main Menu, type **7** to select *Ethernet Statistics*.

The Ethernet Statistics menu in Figure 66 is displayed.

```

Allied Telesyn Ethernet Switch AT-8324 - AT-S25 v2.0.2
Sales
Login Session: Manager                               Module 1 / MASTER

Ethernet Statistics

1 - Display Port Statistics
2 - Display Module Statistics
3 - Clear Module Statistics
4 - Clear Port Statistics

A - Auto Refresh is ON

M - Select another module
R - Return to Previous Menu

Enter your selection?

```

Figure 66 Ethernet Statistics Menu

2. From the Ethernet Statistics menu, type **M** if you wish to select a module other than the one currently displayed.

The prompt message is displayed:

Select Module ID: [1 to 8] ->

3. Enter the ID of the module you wish to select, and press the Enter key.
4. From the Ethernet Statistics menu, type **1** to select *Display Port Statistics*. The Display Port Statistics window in Figure 67 is displayed.

```

Allied Telesyn Ethernet Switch AT-8324 - AT-S25 v2.0.2
Sales
Login Session: Manager                               Module 1 / MASTER

Display Port Statistics
STATISTICS  Port 1  Port 2  Port 3  Port 4  Port 5  Port 6
-----
TX-Total... 0      0      0      0      0      7
RX-Total... 0      0      0      0      0      14067
RX-Ucast... 0      0      0      0      0      130
RX-Bcast... 0      0      0      0      0      8315
RX-Mcast... 0      0      0      0      0      4621
RX-CRC..... 0      0      0      0      0      0
RX-Frag.... 0      0      0      0      0      0
RX-Jabber... 0      0      0      0      0      0
RX-Drop.... 0      0      0      0      0      0
RX-Oversize. 0      0      0      0      0      0

N - Next Page
U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 67 Display Port Statistics Window

Table 16 lists the parameters appeared in the Display Port Statistics and Display Module Statistics windows. These parameters are for viewing purposes only.

Table 16 Port and Module Statistics Parameters

PARAMETER	DESCRIPTION
TX_Total (Transmit Packets)	Number of packets transmitted out the port.
RX_Total (Receive Packets)	Number of packets received on the port.
RX-Ucast (Received Unicast)	Number of unicast packets received on the port.
RX-Bcast (Received Broadcast)	Received Broadcast - Number of broadcast packets received on the port.
Rx-Mcast (Received Multicast)	Received Multicast - Number of multicast packets received on the port.
RX-CRC	Number of packets with a cyclic redundancy check (CRC) error but with the proper length (64-1518 bytes) received on the port.
RX-Frag (Fragmented Packets)	Number of undersized packets, packets with alignment errors, and packets with FCS errors (CRC errors) received on the port.
RX-Jabber	Number of packets received with length greater than <i>MAXFRAMESIZE</i> and <i>invalid CRC</i> .
RX-Drop	Number of received dropped packets.
RX-Oversize	Number of packets exceeding the maximum length of 1518 bytes received on the port (including the CRC) - as specified by IEEE 802.3.
RX-Undersize	Number of packets received on the switch that were less than the minimum length of 64 bytes (including the CRC) - as specified by IEEE 802.3. NOTE: Applies to the Module Statistics only.
RX-Collision	Number of received packets with collision event detected. NOTE: This applies to the Module Statistics only.

- If you wish to clear the counters on the port and return them to "0", type **4** to select *Clear Port Statistics* from the Ethernet Statistics window.

Displaying Switch Statistics

To display Ethernet statistics for an entire switch, perform the following procedure:

1. From the Main Menu, type **7** to select *Ethernet Statistics*.
2. From the Ethernet Statistics menu, type **M** if you wish to select a module other than the one currently displayed.

The prompt message is displayed:

```
Select Module ID: [1 to 8] ->
```

3. Enter the ID of the module you wish to select, and press the Enter key.
4. From the Ethernet Statistics menu, type **2** to select *Display Module Statistics*.

The statistics for the switch are displayed in the Display Module Statistics window, shown in Figure 68.

```

Allied Telesyn Ethernet Switch AT-8324 - AT-S25 v2.0.2
Sales
Login Session: Manager                               Module 1 / MASTER

Display Module Statistics

STATISTICS
-----
TX-Total..... 7
RX-Total..... 14180
RX-Ucast..... 130
RX-Bcast..... 8371
RX-Mcast..... 4662
RX-CRC..... 0
RX-Frag..... 0
RX-Jabber.... 0
RX-Drop..... 0
RX-Oversize.. 0
RX-Undersize. 0
RX-Collision. 0

U - Update Display
R - Return to Previous Menu

Enter your selection? _

```

Figure 68 Display Module Statistics Window

The information in this window is for viewing purposes only. For description of these parameters, refer to Table 16, **Port and Module Statistics Parameters** on page 176.

5. If you wish to clear the counters on the switch and return them to "0", type **3** to select *Clear Module Statistics* from the Ethernet Statistics Menu.

Chapter 14

File Downloads and Uploads

This chapter contains the procedures for displaying and clearing data traffic statistics. Sections in the chapter include:

- ❑ **Obtaining Software Updates** on page 180
- ❑ **Transferring Files from a Local Management Interface** on page 181
- ❑ **Transferring Files Using HyperTerminal Interface** on page 186

There are three files that co-exist on an AT-8316F or an AT-8324 Switch while the device is operating. They are:

- ☐ AT-S25 management software

This is the operating software for the switch.

- ☐ AT-S25 image file

This image contains the code that initially controls the switch whenever you power on or reset the unit.

- ☐ Switch configuration file

This file contains the settings for the different switch parameters, such as VLANs, STP settings, and so forth.

You could use the AT-S25 management software to download new versions of the management software and image file onto a switch so that a switch always has the latest software.

You could also upload a configuration file from a switch onto a management workstation and then download it onto another switch. This can be useful in network environments containing a large number of AT-8316F and/or AT-8324 Switches that will all be configured the same, or nearly the same. What you could do is configure one stack of the AT-8316F or AT-8324 Switches in your network, and then download its configuration file to the other stacks. This can save you the trouble of having to configure each stack individually.

Obtaining Software Updates

Allied Telesyn periodically updates and revises the AT-S25 management software for your AT-8316F and AT-8324 Switches. The latest version of the software is posted on the Allied Telesyn web site for you to download.

New releases of the AT-S25 management software are available from the Allied Telesyn web site at www.alliedtelesyn.com.

Note

All switch models in the AT-8316F or AT-8324 Switch use the same management software image.

Note

For detailed instructions on how to upgrade the AT-S25 Management Software Version 1.5.6.2 or an earlier version to Version 2.0.2, refer to the **Upgrading AT-S25 Version 1.5.6.2 or Earlier to Version 2.0.2 or Later** on page 17.

Transferring Files from a Local Management Interface

This section contains the procedure for downloading or uploading the following files onto a switch from a local management interface.

- ☐ New AT-S25 image file
- ☐ Configuration file

You can transfer a file using Xmodem or TFTP. In order to use TFTP, there must be a node on your network with the TFTP server software and the file to download must be stored on the same node.



Caution

The switch will stop forwarding Ethernet traffic during the download of the AT-S25 software image.

Note

Installing a new AT-S25 software image does not change the current configuration of a switch (e.g., IP address, subnet mask, and virtual LANs). To return a switch to its default configuration values, refer to **Returning the AT-S25 Software to the Factory Default Values** on page 56.

This procedure assumes that you have already obtained the new software from Allied Telesyn and stored it on the management workstation from which you will be performing the procedure, or on the TFTP server.

To download a new software image or configuration file onto a switch, perform the following procedure:

1. Establish a local management interface on the switch where you intend to download the new management software or configuration file.

For instructions, refer to **Starting a Local or Telnet Management Session** on page 34.

2. From the Main Menu, type **4** to select *Administration Menu*.
3. From the Administration Menu, type **D** to select *Downloads & Uploads Menu*.

The Downloads & Uploads Menu in Figure 69 is displayed.

```

Allied Telesyn Ethernet Switch AT-8324 - AT-S25 v2.0.2
Sales
Login Session: Manager                               Module 1 / MASTER

Downloads & Uploads Menu

1 - Download Image through Xmodem/TFTP
2 - Download Configuration through Xmodem/TFTP
3 - Upload Configuration to TFTP Server

S - Save Configuration changes
R - Return to Previous Menu

Enter your selection? _

```

Figure 69 Downloads & Uploads Menu

Downloading An Image File

To download a new image file onto a switch, perform the following procedure:

1. From the Main Menu, type **4** to select *Administration Menu*.
2. From the Administration Menu, type **D** to select *Downloads & Uploads Menu*.
3. To download a new image file onto the switch, type **1** to select *Download Image through Xmodem/TFTP*.

The following prompt is displayed:

Download Method/Protocol [X-Xmodem, T-TFTP]:

- ☐ To download a file using Xmodem, perform the following steps:

- a. Type **X** and press the Enter key. The following prompt is displayed:

The System is now ready for download. Please start your XMODEM transfer.

- b. The file transfer of the new management software image is now begun.

Note

The transfer protocol must be Xmodem or 1K Xmodem. For faster transfer, 1K Xmodem is preferable.

❑ To download a file using TFTP, perform the following procedure:

- a. Type **T** and press the Enter key. The following prompt is displayed:

TFTP Server IP address:

- b. Enter the IP address of the TFTP server. The following prompt is displayed:

Remote File Name:

- c. Enter the directory path and file name of the new management software image that you wish to download; then press the Enter key.

Note

The image file must be stored on the TFTP server.

Once the filename has been specified, the download begins. Downloading an AT-S25 image file can take several seconds.

If you are installing a new management image file, the switch begins to initialize the software after it is installed, a process that takes approximately one minute to complete. Once the management software is initialized, the switch will automatically reboot with the new image file.

When downloading a new management image file using TFTP, this image file is downloaded onto the Master switch of a stack first. Then, from the Master switch, it gets downloaded onto all the Slave switches in the stack. Once this process is finished, the entire stack will reboot with the new image file.

Note

Do not interrupt the initialization process. Do not reboot the switch.

Downloading Configuration File

To download a new configuration file onto a switch, perform the following procedure:

1. From the Main Menu, type **4** to select *Administration Menu*.
2. From the Administration Menu, type **D** to select *Downloads & Uploads Menu*.
3. To download a new configuration file onto the switch, type **2** to select *Download Configuration through Xmodem/TFTP*.

The following prompt is displayed:

```
Download Method/Protocol [X-Xmodem, T-TFTP] :
```

- ☐ To download a file using Xmodem, perform the following steps:

- a. Type **X** and press the Enter key. The following prompt is displayed:

```
The System is now ready for download. Please
start your XMODEM transfer.
```

- b. The file transfer of the new configuration file is now begun.

Note

The transfer protocol must be Xmodem or 1K Xmodem. For faster transfer, 1K Xmodem is preferable.

- ☐ To download a file using TFTP, perform the following procedure:

- a. Type **T** and press the Enter key. The following prompt is displayed:

```
TFTP Server IP address:
```

- b. Enter the IP address of the TFTP server. The following prompt is displayed:

```
Remote File Name:
```

- c. Enter the directory path and file name of the new configuration file that you wish to download; then press the Enter key.

Once the filename has been specified, the download begins. Downloading a configuration file takes only a few moments.

Note

Do not interrupt the initialization process. Do not reboot the switch.

Uploading Configuration File to TFTP Server

To upload a configuration file to the TFTP server on an AT-8316F or an AT-8324 Switch, perform the following procedure:

1. From the Main Menu, type **4** to select *Administration Menu*.
2. From the Administration Menu, type **D** to select *Downloads & Uploads Menu*.
3. To upload a new configuration file onto the switch, type **3** to select *Upload Configuration to TFTP Server*.

The following prompt is displayed:

TFTP Server IP Address :

4. Enter the IP address of the TFTP server. The following prompt is displayed:

Remote File Name:

5. Enter the directory path and file name of the configuration file that you wish to upload; then press the Enter key.

Once the filename has been specified, the upload begins.
Uploading a configuration file takes only a few moments.

Transferring Files Using HyperTerminal Interface

This section contains the procedure for downloading or uploading a file using the Hilgraeve HyperTerminal program.

1. From the HyperTerminal main window, select the *Transfer* menu.
2. Select *Send File* from the Transfer pull-down menu, as shown in Figure 70.

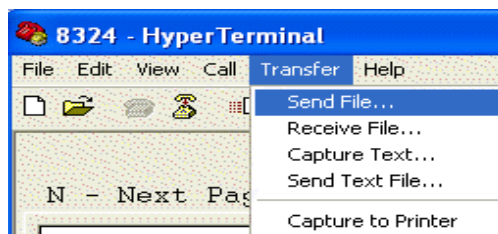


Figure 70 Local Management Window

The Send File window in Figure 71 on page 186 is displayed.

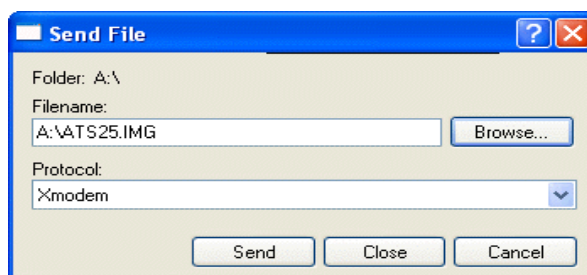


Figure 71 Send File Window

3. Click the Browse button and specify the location and file to be downloaded onto the switch.
4. From the Protocol pull-down menu, select **Xmodem** or **1K XModem** as the transfer protocol. For faster transfer, *1K XModem is preferable*.
5. Click **Send**.

The software immediately begins to download onto the switch. The Xmodem File Send window in Figure 72 displays current status of the software download. The download process takes a couple minutes to complete.

The image shows a Windows-style dialog box titled "Xmodem file send for 8324". It contains several input fields and buttons. The "Sending:" field contains "A:\ATS25.IMG". The "Packet:" field is empty, and the "Error checking:" field contains "CRC". The "Retries:" field contains "0", and the "Total retries:" field contains "0". The "Last error:" field is empty. Below these, the "File:" field is empty, and the "OK of 726K" field contains "OK of 726K". The "Elapsed:" field is empty, the "Remaining:" field is empty, and the "Throughput:" field is empty. At the bottom right, there are two buttons: "Cancel" and "cps/bps".

Figure 72 XModem File Send Window

If you are installing a new management image, the switch begins to initialize the software after it is installed, a process that takes approximately one minute to complete. Once the management software is initialized, the switch automatically resets.

Note

Do not interrupt the initialization process. Do not reboot the switch.

When downloading a new management image file using Xmodem, this image file is downloaded onto the Master switch of a stack first. Then, the Master switch will reboot the entire stack. After the stack reboots, the Master switch will compare the new software version of the new image file with the one used by the Slave switches. If any of the Slave switches has an older software version number, the Master switch will update it with its new management image file. The initialization process will continue once all the Slave switches are upgraded with the new image file.

Section III

Web Browser Management

The chapters in this section explain how to manage the AT-8316F and AT-8324 Fast Ethernet Switches using a web browser. The chapters include:

- ☐ **Chapter 15, Starting a Web Browser Management Interface** on page 189
- ☐ **Chapter 16, Basic Switch Parameters** on page 193
- ☐ **Chapter 17, Port Parameters** on page 206
- ☐ **Chapter 18, Port Security** on page 214
- ☐ **Chapter 19, Port Trunks** on page 216
- ☐ **Chapter 20, Port Mirroring** on page 222
- ☐ **Chapter 21, STP and RSTP** on page 227
- ☐ **Chapter 22, Virtual LANs** on page 242
- ☐ **Chapter 23, MAC Address Table** on page 254
- ☐ **Chapter 24, Class of Service** on page 262
- ☐ **Chapter 25, IGMP Snooping** on page 265

Chapter 15

Starting a Web Browser Management Interface

This chapter contains the procedure for starting a management interface on an AT-8316F or an AT-8324 Switch using a web browser, such as Microsoft® Internet Explorer or Netscape® Navigator.

Web Browser Management Interface

This section explains how to use a web browser management interface.

Starting a Web Browser Interface

Starting a Web browser management interface requires that the Master switch on your network that has an IP address. Once you have started a Web browser management interface on the Master switch, you will have management access to all other AT-8316F and AT-8324 Switches that reside in the same switch.

To start a web browser management interface, perform the following procedure:

1. Start your web browser.

Note

If your PC with the web browser is connected directly to the switch to be managed or is on the same side of a firewall as the switch, you must configure your browser's network options not to use proxies. Consult your web browser's documentation on how to configure the switch's web browser not to use proxies.

2. Enter the IP address of the Master switch in the URL field of the browser, as shown in Figure 73.

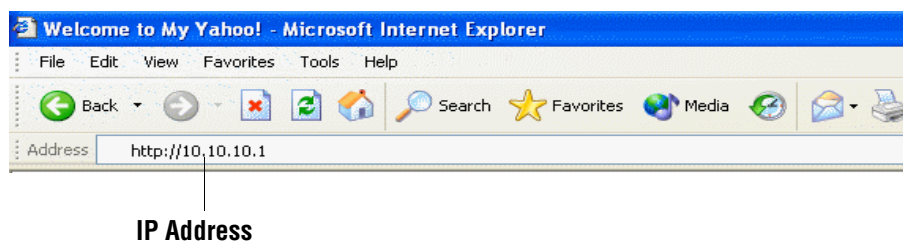


Figure 73 Entering an IP Address in the URL Field

3. When prompted for the user name and password, enter one of the following options.
 - ☐ For Manager access, type **manager** as the user name. The default password is "friend".
 - ☐ For Operator access, type **operator** as the user name. The default password is "operator".

Note

The user names cannot be changed and the passwords are case sensitive. To change a password, refer to **Configuring an IP Address and Switch Name** on page 45.

The window shown in Figure 74 is displayed.

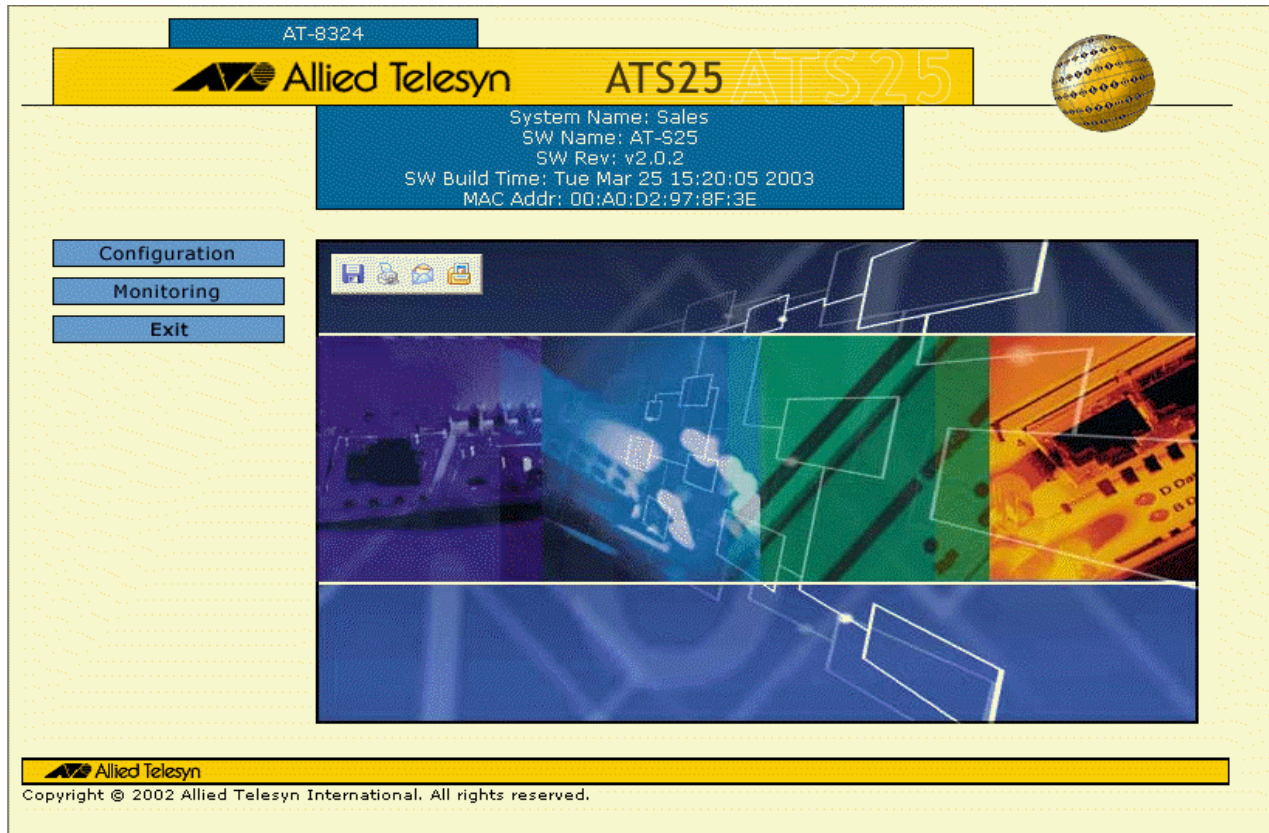


Figure 74 Home Page

This is the Home page of the management software. In the left portion of the Home page is the main menu:

- ☐ Configuration
- ☐ Monitoring
- ☐ Exit

Note

A web browser management interface remains active even if you link to other sites. You could return to the management web pages anytime as long as you do not quit the browser.

Browser Tools

You could use the browser tools to move around the web-browser menus. Selecting **Back** on your browser's toolbar returns you to the previous display. You could also use the browser's **bookmark** feature on frequently-used web-browser menus and windows.

Quitting from a Web Browser Management Interface

To exit from a web browser management interface, perform the following procedure:

1. From any page in AT-S25 management software, select *Exit*. The confirmation window in Figure 75 is displayed.

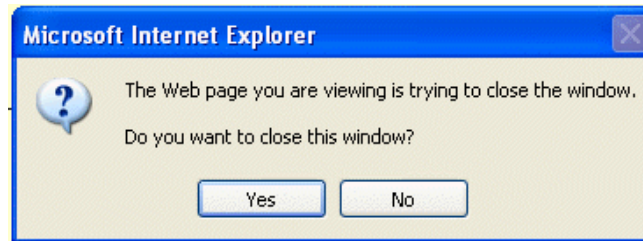


Figure 75 Exit Confirmation Window

2. Type **Y** to exit the web browser management interface or **N** to return to the AT-S25 management software.

Chapter 16

Basic Switch Parameters

This chapter contains the following sections:

- ❑ **Configuring an IP Address and Switch Name** on page 194
- ❑ **Activating the BOOTP and DHCP Services** on page 198
- ❑ **Resetting a Switch** on page 199
- ❑ **Viewing System Information** on page 200
- ❑ **Configuring the SNMP Parameters and Trap IP Addresses** on page 202
- ❑ **Pinging a Remote System** on page 204
- ❑ **Returning the AT-S25 Software to the Factory Default Values** on page 205

Configuring an IP Address and Switch Name

Note

For guidelines on when to assign an IP address, subnet address, and gateway address to an AT-8316F or an AT-8324 Switch, refer to **When Does a Switch Need an IP Address?** on page 42.

To set the basic parameters for an AT-8316F or an AT-8324 Switch, perform the following procedure:

1. From the Home Page, select *Configuration*.

The Configuration window is displayed with the System menu option selected by default.

2. If the System menu option is not selected, select it and then select the *General* tab.

The General window in Figure 76 is displayed.

AT-8324

Configuration

System Name: Sales
SW Name: AT-S25
SW Rev: v2.0.2
SW Build Time: Tue Mar 25 15:20:05 2003
MAC Addr: 00:A0:D2:97:8F:3E

Home

System

Layer 1

Layer 2

Help

Exit

General | SNMP | IGMP | Factory Default

Administration

<p>System Name Sales</p> <p>Administrator </p> <p>Comments </p>	<p>IP Address 149.35.19.153</p> <p>Subnet Mask 255.255.252.0</p> <p>Default Gateway 149.35.16.1</p>
--	--

<p>Manager Password </p> <p>Confirm Manager Password </p>	<p>Operator Password </p> <p>Confirm Operator Password </p>
---	---

Configuration

<p>BOOTP/DHCP <input checked="" type="radio"/> Enable <input type="radio"/> Disable </p> <p>Switch Mode <input type="radio"/> Basic <input checked="" type="radio"/> Tagged </p>	<p>MAC address aging time <input type="text" value="300"/> </p>
--	---

Allied Telesyn
 Copyright © 2002 Allied Telesyn International. All rights reserved.

Figure 76 Configuration - General Window

Note

This procedure only describes the parameters in the Administration section of the window. The parameters in the Configuration and Broadcast Storm Control sections are discussed later in this guide.

Note

The Reset button at the bottom of the window is used to reset the switch.

3. Enter or modify the parameters in the window as desired.

Changes to the parameters take effect immediately on the switch.

Table 17 lists the parameters appeared in the Configuration - General window.

Table 17 Configuration - General Window Parameters

PARAMETER	DESCRIPTION
Administration	
System Name	This parameter specifies a name for the switch (for example, Sales). The value range is 1 to 40 alphanumeric characters. However, setting for this parameter is only optional. NOTE: It is advisable that you assign each switch a name. The names can help you identify the various switches when you manage them and avoid performing a configuration procedure on the wrong switch.
Administrator	This parameter specifies the name of the network administrator responsible for managing the switch. The value range is 1 to 40 alphanumeric characters. However, setting for this parameter is only optional.
Comments	This parameter specifies additional information about the switch, such as its location (e.g., Floor 4, Wiring closet 402B). The range value is 1 to 40 alphanumeric characters. However, setting for this parameter is only optional.
IP Address	This parameter specifies the IP address of the switch. You must specify an IP address if you intend to remotely manage the switch using a web browser, a Telnet utility, or an SNMP management program.
Subnet Mask	This parameter specifies the subnet mask for the switch. You must specify a subnet mask if you assigned an IP address to the switch.

PARAMETER	DESCRIPTION
Default Gateway	This parameter specifies the default router’s IP address. This address is required if you intend to remotely manage the switch from a management station that is separated from the switch by a router.
Manager Password	These parameters are used to change the administrator’s login password for the switch. The password can be from 0 to 20 characters in length. The same password is used for both local and remote management interfaces. To create a new password, enter the new password into both fields. The default password is “friend”. You should not use spaces or special characters, such as asterisks (*) and exclamation points (!), in a password if you will be managing the switch from a web browser. Many web browsers cannot handle special characters in passwords.
Confirm Manager Password	
Operator Password	These parameters are used to change the operator’s login password for the switch. The password can be from 0 to 20 characters in length. The same password is used for both local and remote management interfaces. To create a new password, enter the new password into both fields. The default password is “operator”. You should not use spaces or special characters, such as asterisks (*) and exclamation points (!), in a password if you will be managing the switch from a web browser. Many web browsers cannot handle special characters in passwords.
Operator Confirm Password	
Configuration	
BOOTP/DHCP	Defines whether the switch obtains its IP address from a BOOTP or DHCP server on your network. If this parameter is enabled, the switch obtains its IP address from a BOOTP or DHCP server. For more information on this parameter setting, refer to Activating the BOOTP and DHCP Services on page 198.
Switch Mode	Defines the switch’s current VLAN mode. If this parameter displays “Tagged,” the switch supports port-based and tagged VLANs. If this parameter displays “Basic,” the switch is operating in the Basic VLAN Mode. For more information on this parameter setting, refer to Setting the Switch’s VLAN Mode on page 252.
MAC address aging time	Specifies how long an inactive dynamic MAC address can remain in the MAC Menu before it is deleted. The default is 300 seconds (5 minutes). For more information on this parameter setting, refer to Changing the Aging Time on page 260.

4. Click *Apply*.

Changes are immediately activated on the switch.

Note

A change to any of the above parameters, including the IP address and subnet mask, is immediately activated on the switch.



Caution

A change to the IP address of the switch will result in the loss of the remote management interface. You could restart the management interface using the switch's new IP address.

Activating the BOOTP and DHCP Services

Note

For guidelines or background information on BOOTP and DHCP, refer to the section **Activating the BOOTP and DHCP Services** on page 46.

To activate or deactivate the BOOTP and DHCP protocols on the switch from a web browser management interface, perform the following procedure:

1. From the Home Page, select *Configuration*.

The Configuration window is displayed with the System menu option selected by default.

2. If the System menu option is not selected, select it and then select the *General* tab.

The General window is displayed, as shown in Figure 76 on page 194.

3. In the BOOTP/DHCP options in the General tab window, click either *Enable* or *Disable*.

Note

If you activated BOOTP/DHCP, the switch immediately begins to query the network for a BOOTP or DHCP server. The switch continues to query the network for its IP configuration until it receives a response.

Note

A change to the IP address of the switch will result in the loss of the remote management interface. You could restart the management interface using the switch's new IP address.

Resetting a Switch

To reset a switch, perform the following procedure:

1. From the Home Page, select *Configuration*.

The Configuration window is displayed with the System option selected by default.

2. If the System menu option is not selected, select it and then select the *General* tab.

3. Click *Reset*.

A confirmation prompt is displayed.

4. Click *OK* to reset the switch or *Cancel* to cancel the procedure.

Resetting the switch ends your web browser management interface. You must restart the interface to continue managing the switch.

Viewing System Information

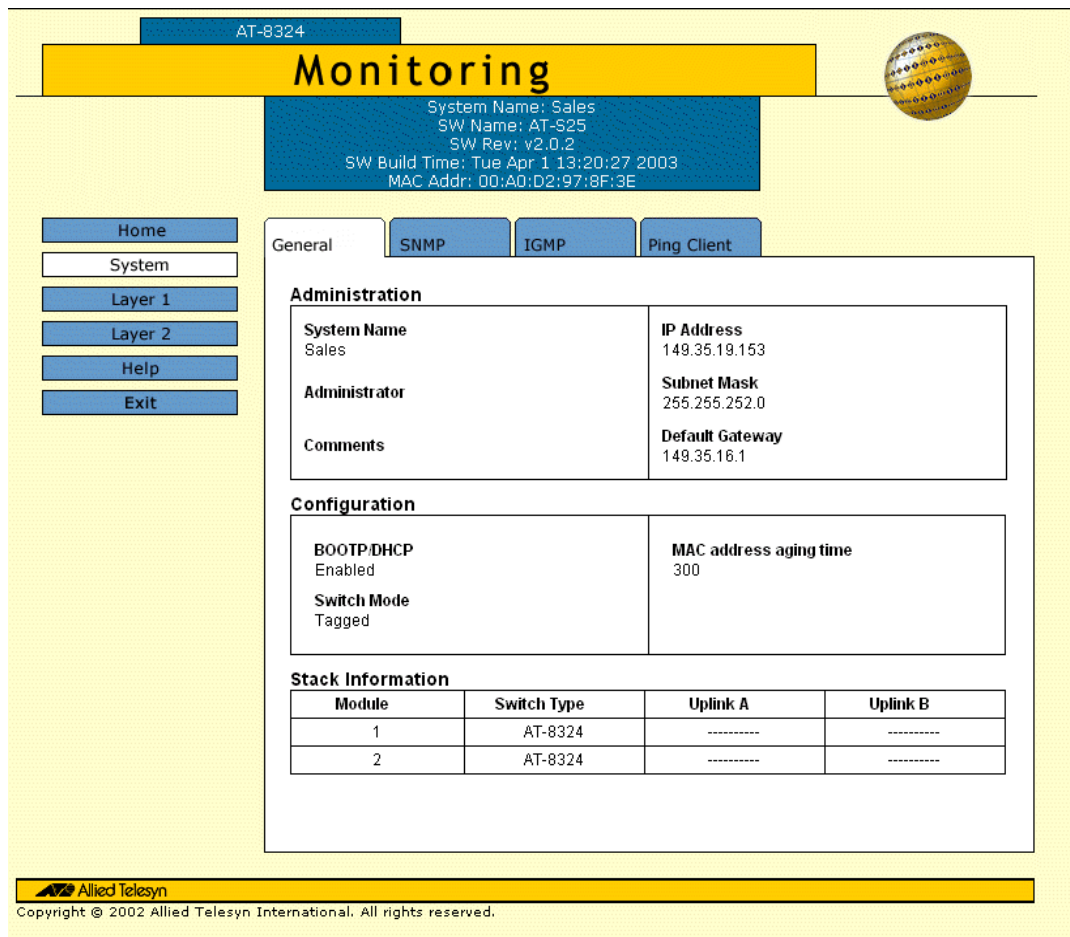
To view basic information about the switch, perform the following procedure:

1. From the Home page, select *Monitoring*.

The Monitoring window is displayed with the System menu option selected by default.

2. If the System menu option is not selected, select it and then select the *General* tab.

The General tab window in Figure 77 is displayed.



AT-8324

Monitoring

System Name: Sales
SW Name: AT-S25
SW Rev: v2.0.2
SW Build Time: Tue Apr 1 13:20:27 2003
MAC Addr: 00:A0:D2:97:8F:3E

Home
System
Layer 1
Layer 2
Help
Exit

General | SNMP | IGMP | Ping Client

Administration

System Name Sales	IP Address 149.35.19.153
Administrator	Subnet Mask 255.255.252.0
Comments	Default Gateway 149.35.16.1

Configuration

BOOTP/DHCP Enabled	MAC address aging time 300
Switch Mode Tagged	

Stack Information

Module	Switch Type	Uplink A	Uplink B
1	AT-8324	-----	-----
2	AT-8324	-----	-----

Allied Telesyn
Copyright © 2002 Allied Telesyn International. All rights reserved.

Figure 77 Monitoring - General Window

Table 18 lists the parameters appeared in the Monitoring - General window. The parameters in this window are for viewing purposes only. You could not change any of the values from this window.

Table 18 Monitoring - General Window Parameters

Section	DESCRIPTION
Administration	<p>This section contains a variety of information as listed below:</p> <ul style="list-style-type: none"> • System Name • Administrator • Comments • IP Address • Subnet Mask • Default Gateway <p>These parameters are defined in the procedure Configuring an IP Address and Switch Name on page 194, which also explains how to change the parameters.</p>
Configuration	<p>This section contains the following items:</p> <ul style="list-style-type: none"> • BOOTP/DHCP • Switch Mode • MAC address aging time
Stack Information	<p>This section contains the following information:</p> <ul style="list-style-type: none"> • Module Information • Switch Type

Configuring the SNMP Parameters and Trap IP Addresses

To change the switch's SNMP community strings or to specify the IP addresses of management stations to receive traps from the switch, perform the following procedure:

1. From the Home page, select *Configuration*.

The Configuration window is displayed with the System menu option selected by default.

2. If the System menu option is not selected, select it and then select the *SNMP* tab.

The SNMP window in Figure 78 is displayed.

AT-8324

Configuration

System Name: Sales
SW Name: AT-S25
SW Rev: v2.0.2
SW Build Time: Tue Mar 25 15:20:05 2003
MAC Addr: 00:A0:D2:97:8F:3E

Home System Layer 1 Layer 2 Help Exit

General **SNMP** IGMP Factory Default

☐ Enable SNMP Access

Community	Trap Receiver (IP Address)
Get Community public	Trap Receiver 1 0 . 0 . 0 . 0
Set Community private	Trap Receiver 2 0 . 0 . 0 . 0
Trap Community public	Trap Receiver 3 0 . 0 . 0 . 0
	Trap Receiver 4 0 . 0 . 0 . 0

Apply

Allied Telesyn
Copyright © 2002 Allied Telesyn International. All rights reserved.

Figure 78 Configuration - SNMP Window

3. Enter or modify the parameters as desired.

To change a value, type its corresponding number and, when prompted, enter the new value.

- ☐ To set a switch's SNMP community strings, use the parameters described below:
 - ◆ GET Community
 - ◆ SET Community
 - ◆ TRAP Community

- ❑ To specify the IP addresses of up to four management workstations on your network to receive traps from the switch, use the selections below:
 - ◆ Trap Receiver 1
 - ◆ Trap Receiver 2
 - ◆ Trap Receiver 3
 - ◆ Trap Receiver 4

Note

The Enable SNMP Access check box the window controls whether the switch can be remotely managed using an SNMP application program. If the check box is empty, the switch cannot be managed through SNMP. This is the default.

4. Click *Apply*.

Changes are immediately activated on the switch.

Note

For instructions on configuring IGMP Snooping using the web browser, refer to Chapter 25, **IGMP Snooping** on page 265.

Pinging a Remote System

You could instruct the switch to ping a node on your network. This procedure is useful in determining whether a valid link exists between the switch and another device.

To ping a network device, perform the following procedure:

1. From the Home Page, select *Monitoring*.

The Monitoring window is displayed with the System menu option selected by default.

2. If the System menu option is not selected, select it and then select the *Ping Client* tab.

The window in Figure 79 is displayed.

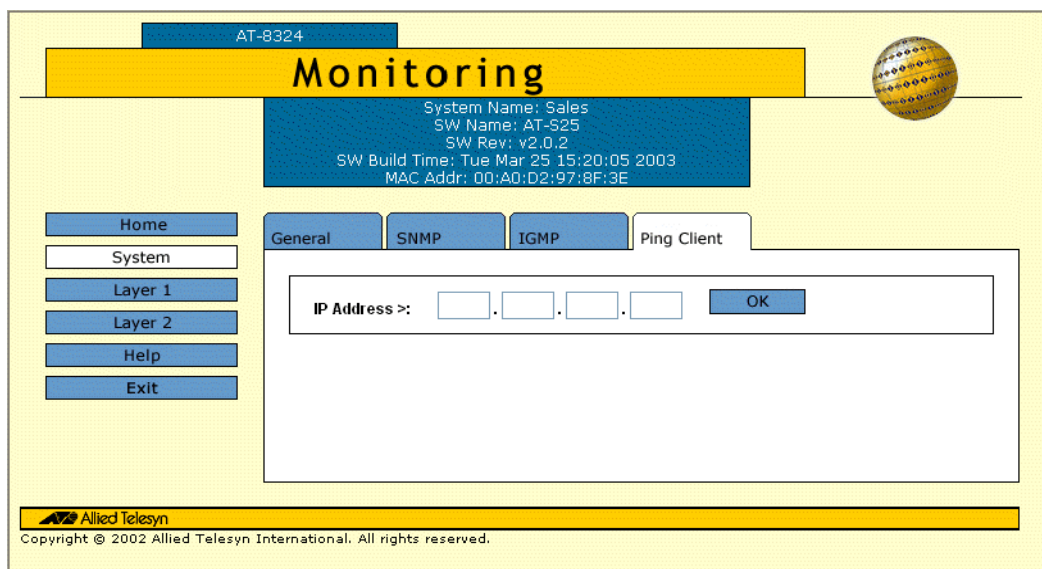


Figure 79 Monitoring - Ping Client Window

3. Enter the IP address of the end node you wish the switch to ping.
4. Click *OK*.

The results of the ping are displayed in a new window.

5. To stop the pinging, click *OK* in the pinging window.

Returning the AT-S25 Software to the Factory Default Values

The procedure in this section returns all AT-S25 software parameters, except the IP address, subnet mask, and gateway address, to their default values. This procedure also deletes any VLANs that you have created on the switch.

Note

The AT-S25 software default values can be found in **Appendix A, AT-S25 Default Settings** on page 272.

To return the AT-S25 management software to its default settings, perform the following procedure:

1. From the Home Page, select *Configuration*.

The Configuration window is displayed with the System menu option selected by default.

2. If the System menu option is not selected, select it and then select the *Factory Default* tab.

The Factory Default tab in Figure 80 is displayed.

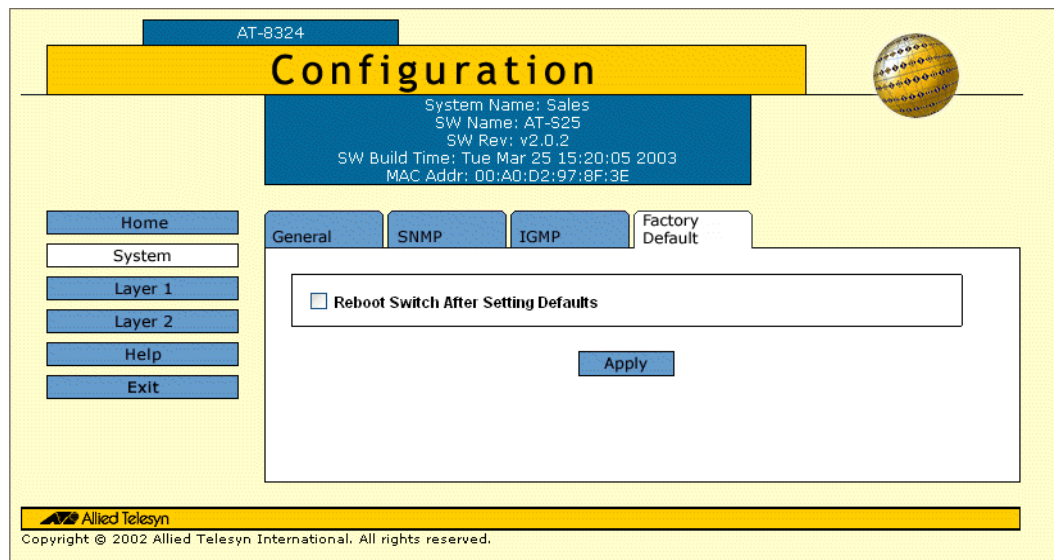


Figure 80 Configuration - Factory Default Window

3. Click the check box next to Reboot Switch After Setting Defaults.
4. Click *Apply*.
5. Follow the prompts.

Chapter 17

Port Parameters

The procedures in this chapter allow you to view and change the parameter settings for the individual ports on a switch. Examples of port parameters that you could adjust include duplex mode and port speed.

This chapter contains the following procedures:

- ❑ **Configuring Port Parameters** on page 207
- ❑ **Displaying Port Status and Statistics** on page 210

Configuring Port Parameters

To configure the parameter settings for a port on a switch, perform the following procedure:

1. From the Home page, select *Configuration*.
2. From the Configuration page, select *Layer 1*.
3. Select the *Port Setting* tab.

The Port Settings window is shown in Figure 81.

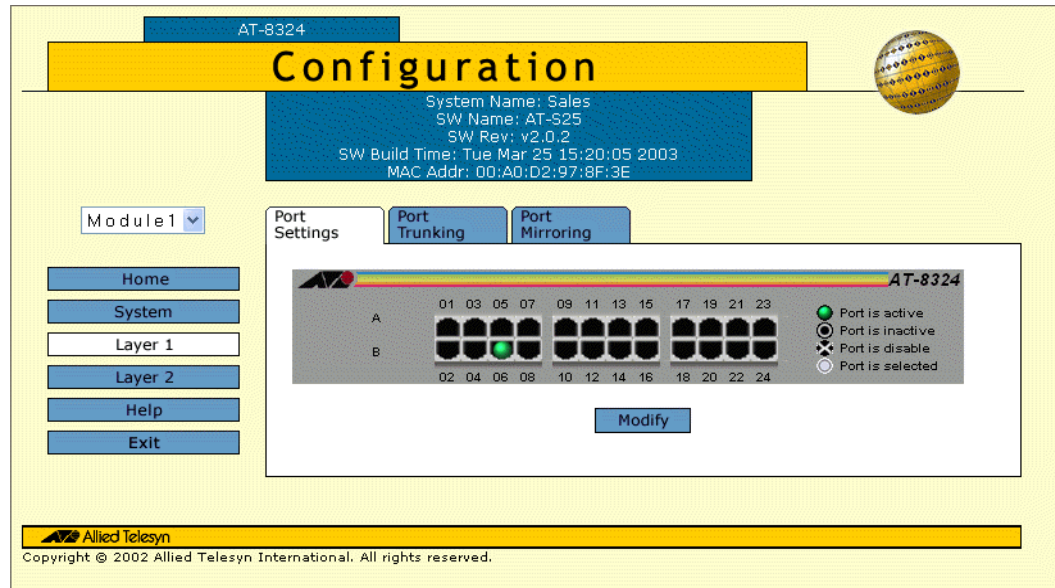


Figure 81 Configuration - Port Settings Window

A graphical image of an AT-8316F or an AT-8324 Fast Ethernet Switch is displayed.

4. Select a port that you wish to configure.
The selected port turns white. You could select more than one port at a time to configure. (To deselect a port, click it again.)
5. Click *Modify*.

The Settings for Port window is displayed. An example of the window is shown in Figure 82.

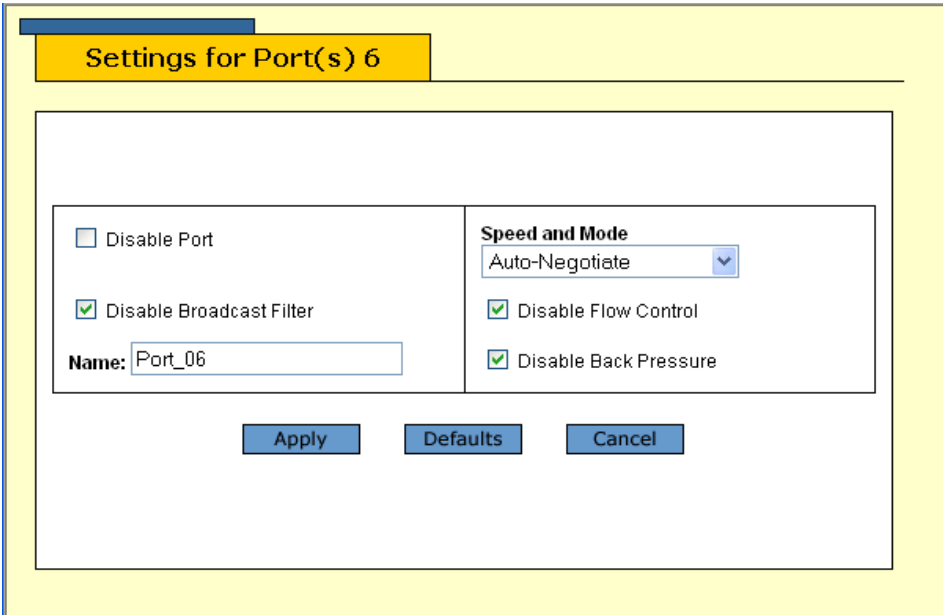


Figure 82 Example of Settings for Port(s) Window

Note
Clicking *Default* returns the port settings to the default values. Default values are listed in **Appendix A, AT-S25 Default Settings** on page 272.

6. Enter or modify the port parameters as desired.
- Table 19 lists the parameters appeared in the Settings for Port window.

Table 19 Port Setting Parameters

Parameter	DESCRIPTION
Disable Port	Enables or disables a port. A disabled port will not accept or transmit frames. Possible settings for this parameter are: <ul style="list-style-type: none">• Disable• Enable (default)
Disable Broadcast Filter	Enables or disables the broadcast filter for the selected port. Possible settings for this parameter are: <ul style="list-style-type: none">• Disable (default)• Enable

Parameter	DESCRIPTION
Speed and Mode	<p>Configures the operating speed and duplex mode of the selected port.</p> <p>Possible settings for this parameter are:</p> <ul style="list-style-type: none"> • Auto-Negotiate: Allows the port to automatically negotiate with the device connected to it (default). • 10Mbps - Half Duplex • 10Mbps - Full Duplex • 100Mbps - Half Duplex • 100Mbps - Full Duplex
Disable Flow Control	<p>Uses a special pause packet to stop the end node from sending frames. The pause packet notifies the end node to stop transmitting for a specified period of time.</p> <p>Possible settings for this parameter are:</p> <ul style="list-style-type: none"> • Enable • Disable (default) <p>NOTE: This parameter only applies to ports operating in full-duplex mode.</p>
Disable Back Pressure	<p>Uses a special packet to halt the transmission of the JAM pattern if there is a pending packet for transmission while the port is transmitting the JAM pattern.</p> <p>Possible settings for this parameter are:</p> <ul style="list-style-type: none"> • Enable • Disable (default) <p>If you select "Enable" when the port is running "half-duplex" mode and the number of packets received exceed the received threshold of the port (which is 160 for 10/100 port, and 664 for 1 Gig port), the port will transmit a JAM pattern for a short amount of time.</p> <p>NOTE: This parameter only applies to the port that is in half-duplex mode.</p>

7. Click *Apply*.

Changes are immediately activated on the switch.

Displaying Port Status and Statistics

The procedure in this section displays the operating status of the ports on a switch and port statistics. You could view a port's operating speed, duplex mode, and more. You could also view the operating status of any GBIC modules installed in an AT-8324.

To display the status or statistics of a switch port, perform the following procedure:

1. From the Home page, select *Monitoring*.
2. From the Monitoring page, select *Layer 1*.
3. Select the *Port Settings* tab. The tab is shown in Figure 83.

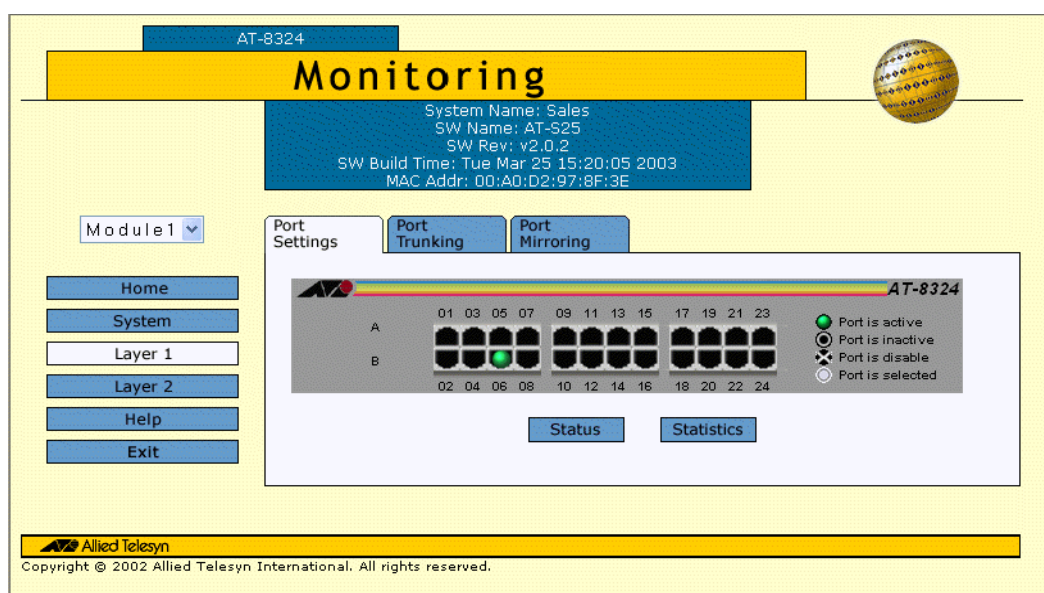


Figure 83 Port Monitoring Page

A graphical image of an AT-8316F or an AT-8324 Fast Ethernet Switch is displayed. Ports with valid links to end nodes contain a green light.

4. Select a port. You could select more than one port at a time when you wish to display port status. However, you could select only one port when displaying statistics.

A selected port turns white. (To deselect a port, click it again.)

5. Click *Status* to display the port's operating status or *Statistics* to display port statistics.

If you select *Port Status*, the Port Status window in Figure 84 is displayed.

Port Status - Port(s) 6

Total Port(s) Selected: 1. Page 1 of 1

PortName/UplinkType	State	Nego	Link	Speed	Duplex	PVID	FlowCtrl	STP_State
Port_06	Enable	Auto	Up	100MB	Half	0001	Disable	-----

OK

Figure 84 Port Status Window

The information in this window is for viewing purposes only. To adjust port parameters, refer to **Configuring Port Parameters** on page 207.

Table 20 lists the parameters appeared in the Port Status window.

Table 20 Port Status Parameters

PARAMETER	DESCRIPTION
PortName/ UplinkType	PortName is the name of the port, and UplinkType is the type of the applique' in the uplink slot (AT-A14, AT-A15, AT-A17, AT-A18, or AT-A19). NOTE: The UplinkType only applies to the uplink ports.
State	The current state of the port. Possible settings for this parameter are: <ul style="list-style-type: none"> • Enable (default) • Disable

PARAMETER	DESCRIPTION
Nego	<p>The status of Auto-Negotiation on the port.</p> <p>Possible settings for this parameter are:</p> <ul style="list-style-type: none"> • Auto - Indicates that the port is using Auto-Negotiation to set operating speed and duplex mode. • Manual - Indicates that the operating speed and duplex mode have been set manually.
Link	<p>The status of the link between the port and the end node connected to the port.</p> <p>Possible settings for this parameter are:</p> <ul style="list-style-type: none"> • Up - indicates that a valid link exists between the port and the end node. • Down - indicates that the port and the end node have not established a valid link.
Speed	<p>The operating speed of the port.</p> <p>Possible settings for this parameter are:</p> <ul style="list-style-type: none"> • 10 Mbps = 10 MB • 100 Mbps = 100 MB • 1000 Mbps = 1 GB (AT-8324 uplink only)
Duplex	<p>The duplex mode of the port.</p> <p>Possible settings for this parameter are:</p> <ul style="list-style-type: none"> • Half-duplex • Full-duplex
PVID	<p>The port VLAN identifier currently assigned to the port.</p>
FlowCtrl	<p>The flow control setting for the port.</p> <p>Possible settings for this parameter are:</p> <ul style="list-style-type: none"> • Enable • Disable
STP_State	<p>The current operating status of the port.</p> <p>Possible settings for this parameter are:</p> <ul style="list-style-type: none"> • Disable • Blocking • Listening • Learning • Forwarding

If you select Statistics, the Statistics window in Figure 85 is displayed.

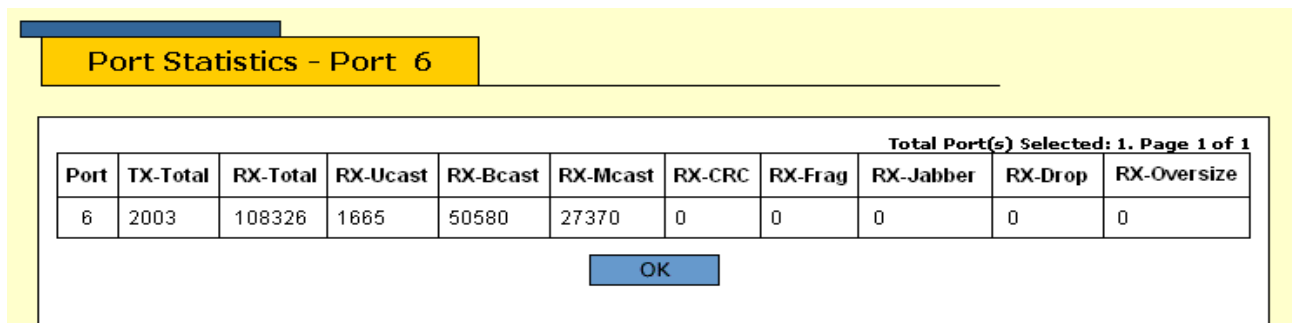


Figure 85 Port Statistics Window

Table 21 lists the parameters appeared in the Port Statistics window.

Table 21 Port Statistics Parameters

PARAMETER	DESCRIPTION
Port	Number of the selected port.
TX-Total	Number of bytes transmitted out the port.
RX-Total	Number of bytes received on the port.
RX-Ucast	Number of unicast packets received on the port.
RX-Bcast	Received Broadcast - Number of broadcast packets received on the port.
Rx-Mcast	Received Multicast - Number of multicast packets received on the port.
RX-CRC	Number of packets with a cyclic redundancy check (CRC) error but with the proper length (64-1518 bytes) received on the port.
RX-Frag	Number of undersized packets, packets with alignment errors, and packets with FCS errors (CRC errors) received on the port.
RX-Jabber	Number of Jabber packets received. A Jabber packet is a packet which has its length greater than <i>MAXFRAMESIZE</i> , <i>invalid CRC</i> , and <i>Rx error event has been detected</i> .
RX-Drop	Number of dropped packets.
RX-Oversize	Number of packets exceeding the maximum specified by IEEE 802.3 (1518 bytes including the CRC) received on the port.

Chapter 18

Port Security

This chapter explains how to display the current port security level on the switch from a web browser management interface.

Note

For background information on port security, refer to **Port Security Overview** on page 68.

Note

A switch's port security level can be changed only from a local management interface.

Displaying the Port Security Level

To display the switch's port security level, perform the following procedure:

1. From the Home page, select *Monitoring*.
2. From the Configuration page, select *Layer 2*.
3. From the Layer 2 page, select the *Port Security* tab.

The current security level is displayed.

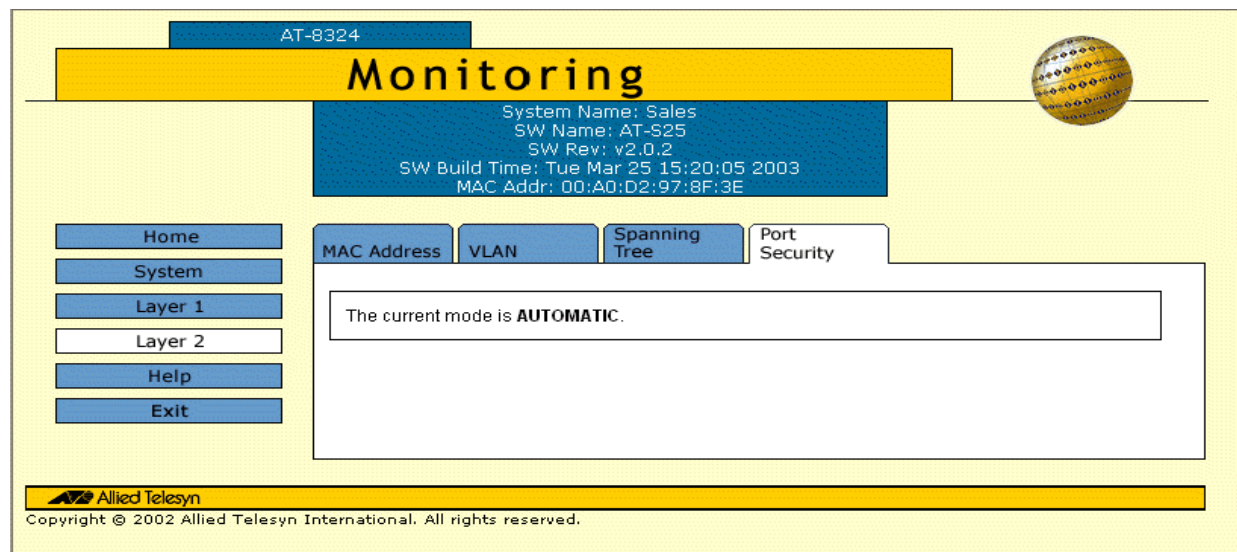


Figure 86 Port Security Menu

Chapter 19

Port Trunks

This chapter contains the procedure for creating or deleting a port trunk from a web browser management session.

Note

For background information and guidelines on port trunking, refer to **Port Trunking Overview** on page 78.

This chapter contains the following procedures:

- ❑ **Creating a Port Trunk** on page 217
- ❑ **Modifying a Port Trunk** on page 219
- ❑ **Deleting a Port Trunk** on page 220
- ❑ **Displaying Port Trunks** on page 221

Creating a Port Trunk



Caution

Do not connect the cables of a port trunk to the ports on the switch until after you have configured the ports on both the switch and the end node. Connecting the cables prior to configuring the ports can create loops in your network topology, which can result in broadcast storms and poor network performance.

To create a port trunk, perform the following procedure:

1. From the Home page, select *Configuration*.
2. From the Configuration page, select *Layer 1*.
3. Select the *Port Trunking* tab.

The Port Trunking tab window in Figure 87 is displayed.

Figure 87 Port Trunking Tab Window

4. Select the Module pull-down list and choose the switch where you want to create the port trunk.
5. Click *Create*.

The Port Trunking window is displayed in Figure 88. The graphic image of the switch will differ depending on the switch model.

Figure 88 Port Trunking Window - Create

6. Select the Trunk Number pull-down list and choose the port group where you want to create the port trunk.
 7. In the Trunk Name text box, enter a name for the new trunk. The name can be from one to ten alphanumeric characters.
 8. Click the ports in the graphic switch image that you want to comprise the port trunk. A selected port turns white. To deselect a port, click it again.
 9. Click *Apply*.
 10. Configure the ports on the remote switch for port trunking.
 11. Connect the cables to the ports of the trunk on the switch.
- The port trunk is ready for network operation.

Modifying a Port Trunk

To modify a port trunk, perform the following procedure:

1. From the Home page, select *Configuration*.
2. From the Configuration page, select *Layer 1*.
3. Select the *Port Trunking* tab. The Port Trunking tab window in Figure 87 on page 217 is displayed.
4. Select the Module pull-down list and choose the switch in the stack with the port trunk you want to modify.
5. Click the circle next to the number of the trunk you want to modify. You can select only one port trunk at a time.
6. Click *Modify*.

The Port Trunking window in Figure 89 is displayed.

The screenshot shows the 'Port Trunking' window. At the top, there is a yellow header bar with the text 'Port Trunking'. Below this, the window is divided into two main sections. The left section is labeled 'Trunk Number # 1 (Port 1 - Port 8)' and is currently empty. The right section is labeled 'Trunk Name:' and contains a text box with the value 'Sales_Trunk'. Below these sections, there is a note: 'Please select ports within range only'. Underneath the note is a graphic representation of a switch with 24 ports, labeled A and B. Ports 01 through 24 are shown in a grid. Ports 01, 03, 05, 07, 09, 11, 13, 15, 17, 19, 21, and 23 are currently selected (white). Ports 02, 04, 06, 08, 10, 12, 14, 16, 18, 20, 22, and 24 are currently unselected (black). To the right of the port grid, there are two radio buttons: 'Port included in Trunk' (selected) and 'Port not included in Trunk'. At the bottom of the window, there are two buttons: 'Apply' and 'Cancel'.

Figure 89 Example of Port Trunking Window - Modify

7. To change the trunk name, select the Trunk Name text box and enter the new name.
8. To add or remove ports from the trunk, click the ports in the graphic switch image. A selected port turns white. To remove a port, click it to change it to black.

New ports added to a trunk must reside in the same port group as the original ports.

9. Click *Apply*.

Changes to the port trunk are immediately activated on the switch. You can now connect the data cables to the ports of the trunk on the switch.

Deleting a Port Trunk



Caution

Disconnect the cables from the port trunk on the switch before performing the following procedure. Deleting a port trunk without first disconnecting the cables can create loops in your network topology, which can result in broadcast storms and poor network performance.

To delete a port trunk, perform the following procedure:

1. From the Home page, select *Configuration*.
2. From the Configuration page, select *Layer 1*.
3. Select the *Port Trunking* tab.
The Port Trunking tab window in Figure 87 on page 217 is displayed with the configuration of previously created trunks.
4. Select the Module pull-down list and choose the switch in the stack with the port trunk you want to modify.
5. Click the circle next to the number of the trunk you want to modify. You can select only one port trunk at a time.
6. Click *Remove*.

A confirmation prompt is displayed.

Click OK to delete the port trunk or Cancel to cancel the procedure.

Displaying Port Trunks

To display the port trunks on a switch, do the following:

1. From the Home page, select *Configuration* or *Monitoring*.
2. Select *Layer 1*.
3. Select the *Port Trunking* tab.
4. Select the Module pull-down list and choose the switch in the stack with the port trunks you want to view.

Chapter 20

Port Mirroring

This chapter contains the procedures for creating and deleting a port mirror.

Note

For background information on port mirroring, refer to **Port Mirroring Overview** on page 89.

This chapter contains the following procedures:

- ❑ **Creating a Port Mirror** on page 223
- ❑ **Deleting a Port Mirror** on page 225
- ❑ **Viewing Source and Destination Ports** on page 226

Creating a Port Mirror

To create a port mirror, perform the following procedure:

1. From the Home page, select *Configuration*.
2. From the Configuration page, select *Layer 1*.
3. Select the *Port Mirroring* tab.

The Port Mirroring window in Figure 90 is displayed.

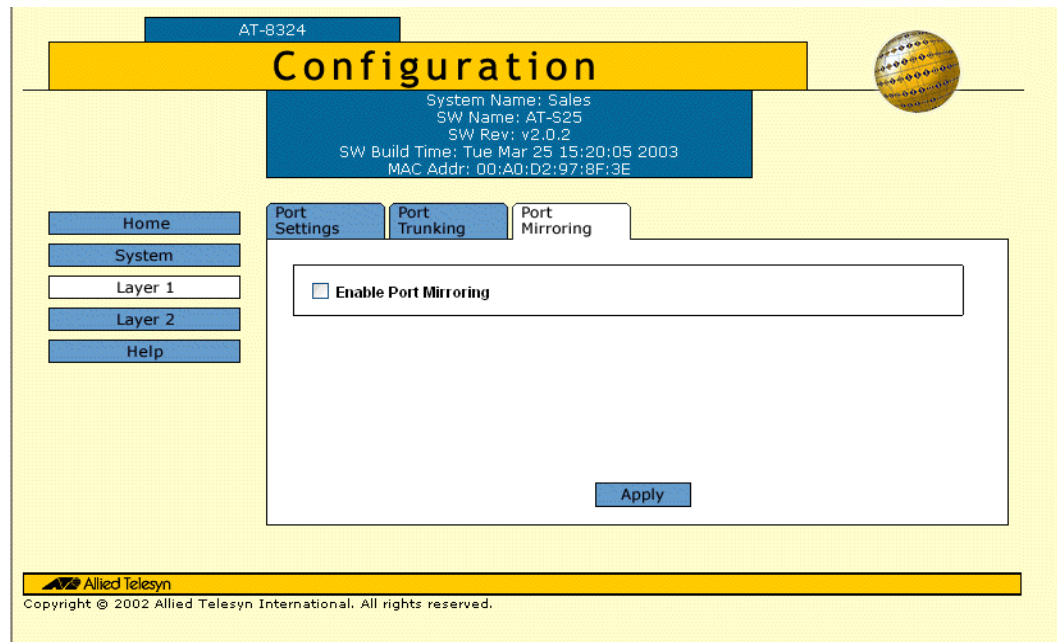


Figure 90 Port Mirroring Window

4. Click the *Enable Port Mirroring* check box.
5. Click *Apply*.

New selections appear in the Port Mirroring window, as shown in Figure 91.

Figure 91 Port Mirroring Window

6. Use the Destination Module and Port pull-down menus to select the destination port. This is the port where the network analyzer will be located.
7. Use the Source Module and Port pull-down menus to select the source port. This is the port whose traffic is to be copied to the destination port.
8. Click *Apply*.

The port mirror is immediately activated. You can now connect a data analyzer to the destination port to monitor the traffic on the source port.

Deleting a Port Mirror

To delete a port mirror, perform the following procedure:

1. From the Home page, select *Configuration*.
2. From the Configuration page, select *Layer 1*.
3. Select the *Port Mirroring* tab.

The Port Mirroring window in Figure 91 on page 224 is displayed.

4. Click the *Enable Port Mirroring* check box. This removes the check from the box.
5. Click *Apply*.

Port mirroring is now disabled on the stack. The port that was functioning as the destination port can now be connected to an end node for normal network operations.

Viewing Source and Destination Ports

To view the source and destination ports of a port mirror, do the following:

1. From the Home page, select *Configuration* or *Monitoring*.
2. Select *Layer 1*.
3. Select the *Port Mirroring* tab.

The Port Mirroring window in Figure 91 on page 224 is displayed.

Chapter 21

STP and RSTP

This chapter explains how to configure the STP and RSTP parameters from a web browser management interface.

Sections in the chapter include:

- ☐ **Enabling or Disabling STP or RSTP** on page 228
- ☐ **Configuring STP** on page 233
- ☐ **Displaying STP Status and Settings** on page 235
- ☐ **Configuring RSTP** on page 237
- ☐ **Displaying RSTP Status and Settings** on page 240

Note

For background information on rapid spanning tree, refer to **STP and RSTP Overview** on page 93.

Enabling or Disabling STP or RSTP

An AT-8300 Series stack can support STP and RSTP. Only one spanning tree protocol can be active on a stack at a time. Before you can enable a spanning tree protocol, you must first select it as the active spanning tree protocol. Once selected, you can then enable or disable it.

To select the active spanning tree protocol and to enable or disable it, perform the following procedure:

1. From the Home page, select *Configuration*.
2. From the Configuration page, select *Layer 2* tab.
3. From the Layer 2 page, select the *Spanning Tree* tab.

The Spanning Tree window in Figure 92 is displayed.

The screenshot shows the AT-8324 Configuration page. At the top, a yellow banner reads "Configuration". Below it, system information is displayed: System Name: Sales, SW Name: AT-S25, SW Rev: v2.0.2, SW Build Time: Tue Mar 25 15:20:05 2003, and MAC Addr: 00:A0:D2:97:8F:3E. On the left, a navigation menu includes Home, System, Layer 1, Layer 2 (selected), Help, and Exit. The main content area has tabs for MAC Address, VLAN, COS, and Spanning Tree (selected). In the Spanning Tree section, there is a checkbox for "Enable Spanning Tree" (unchecked), an "Active Protocol Version" section with radio buttons for STP and RSTP (RSTP is selected), and an "Apply" button. Below this is an "RSTP Configuration" section with a "Configure" button. The footer includes the Allied Telesyn logo and copyright information: Copyright © 2002 Allied Telesyn International. All rights reserved.

Figure 92 Configuration - Spanning Tree Window

4. To change the active spanning tree protocol on the switch, click *STP* or *RSTP* in the Active Protocol Version section of the window. The default is RSTP.
5. To enable or disable spanning tree, click the *Enable Spanning Tree* check box. A check indicates that the feature is enabled while no check indicates that the feature is disabled. The default is disabled.

Note

Only one spanning tree protocol can be active on a stack at a time.

6. Click *Apply*.
7. If you activated STP, go to **Configuring STP** on page 233.
8. If you activated RSTP, go to **Configuring RSTP** on page 237.

STP and RSTP Parameters

Since both STP and RSTP are sharing the same parameters; instead of having them listed by sections in this chapter, they are now listed in the Table 22 below:

Note

A change to parameter will take effect on both protocols.

Table 22 STP and RSTP Parameters

PARAMETER	DESCRIPTION
Force Version	<p>This selection determines whether the bridge will operate with RSTP or in an STP-compatible mode.</p> <ul style="list-style-type: none"> If you select <i>RSTP</i>, the bridge operates all ports in RSTP, except for those ports that receive STP BPDU packets. If you select <i>Force STP Compatible</i>, the bridge operates in RSTP, using the RSTP parameter settings, but it sends out only STP BPDU packets from the ports.
Bridge Priority	<p>The priority number for the bridge. This number is used in determining the root bridge. The bridge with the lowest priority number is selected as the root bridge. If two or more bridges have the same priority value, the bridge with the numerically lowest MAC address becomes the root bridge. When a root bridge goes off-line, the bridge with the next priority number automatically takes over as the root bridge.</p> <p>This parameter has a range of from 0 (zero) to 61,440 in increments of 4096, with 0 being the highest priority. For a list of the increments, refer to Table 6, Bridge Priority Value Increments on page 94.</p>
Bridge Hello Time	<p>The time interval between generating and sending configuration messages by the bridge.</p> <p>This parameter has a range of from 1 to 10 seconds. The default is 2 seconds.</p>
Bridge Forwarding	<p>The waiting period before a bridge changes to a new state, for example, becomes the new root bridge after the topology changes. If the bridge transitions too soon, not all links may have yet adapted to the change, possibly resulting in a network loop.</p> <p>This parameter has a range of from 4 to 30 seconds. The default is 15 seconds.</p>

Table 22 STP and RSTP Parameters

PARAMETER	DESCRIPTION
Bridge Max Age	<p>The length of time after which stored bridge protocol data units (BPDUs) are deleted by the bridge. All bridges in a bridged LAN use this aging time to test the age of stored configuration messages called BPDUs.</p> <p>For example, if you use the default 20, all bridges delete current configuration messages after 20 seconds. This parameter can be from 6 to 40 seconds. The default is 20 seconds.</p> <p>In selecting a value for maximum age, the following must be observed:</p> <ul style="list-style-type: none"> • MaxAge must be more then $[2 \times (\text{HelloTime} + 1)]$ • MaxAge must be less then $[2 \times (\text{ForwardingDelay} - 1)]$
Bridge Identifier	<p>The MAC address of the bridge. The bridge identifier is used as a tie breaker in the selection of the root bridge when two or more bridges have the same bridge priority value.</p> <p>This value cannot be changed.</p>
Root Bridge	The MAC address of the bridge functioning as the root bridge in the spanning tree domain. This value is for viewing purposes only and cannot be changed.
Root Priority	The priority number of the root bridge.
Port Priority or Priority	<p>This parameter is used as a tie breaker when two or more ports are determined to have equal costs to the root bridge. The range is 0 to 240 in increments of 16. The default value is 8 (priority value 128).</p> <p>For a list of the increments, refer to Table 8, Port Priority Value Increments on page 96.</p>
Port Cost or Cost	<p>The spanning tree algorithm uses the cost parameter to decide which port provides the lowest cost path to the root bridge.</p> <p>For an explanation of this parameter, refer to Table 7, Auto-Detect Port Costs on page 95.</p>
Point-to-Point or P2P	<p>This parameter defines whether the port is functioning as a point-to-point port.</p> <p>This parameter applies only to RSTP. For an explanation of this parameter, refer to Point-to-Point Ports and Edge Ports on page 98.</p>

Table 22 STP and RSTP Parameters

PARAMETER	DESCRIPTION
Edge Port	<p>This parameter defines whether the port is functioning as an edge port.</p> <p>This parameter applies only to RSTP. For an explanation of this parameter, refer to Point-to-Point Ports and Edge Ports on page 98.</p>
Port	The port number.
Enable	The port link status.
State	The current state of the selected port.
Role	<p>The current role of the selected port.</p> <p>The settings for this parameter are:</p> <ul style="list-style-type: none"> • Root Port • Alternate • Designated • Backup
Version	<p>The version of the BPDU.</p> <p>The settings for this parameter are:</p> <ul style="list-style-type: none"> • STP • RSTP

Configuring STP

Configuring a Bridge's STP Settings

This section contains the procedure for configuring a bridge's STP settings.



Caution

The bridge provides default STP parameters that are adequate for most networks. Changing them without prior experience and an understanding of how STP works might have a negative effect on your network. You should consult the IEEE 802.1d standard before changing any of the STP parameters.

To configure STP, perform the following procedure:

1. From the Spanning Tree window in Figure 92 on page 228, click *Configure*.

The STP Configuration Spanning Tree window is displayed in Figure 92.

AT-8324

Configuration

System Name: Sales
SW Name: AT-S25
SW Rev: v2.0.2
SW Build Time: Tue Apr 1 13:20:27 2003
MAC Addr: 00:A0:D2:97:8F:3E

Module1 ▾

Home
System
Layer 1
Layer 2
Help
Exit

MAC Address | VLAN | COS | Spanning Tree

Bridge Identifier
00:A0:D2:97:8F:3E

Bridge Priority [0-15]
8 * 4096 = 32768

Bridge Hello Time [1 - 10]
2

Bridge Forwarding Delay [4 - 30]
15

Bridge Max Age [6 - 40]
20

Apply Defaults

AT-8324

	01	03	05	07	09	11	13	15	17	19	21	23
A	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
B	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	02	04	06	08	10	12	14	16	18	20	22	24

Port is not selected
Port is selected

Modify
Back

Allied Telesyn
Copyright © 2002 Allied Telesyn International. All rights reserved.

Figure 93 STP Configuration Spanning Tree Window

- 2. Enter or modify the STP configuration settings as desired.
For descriptions of the parameters, refer to Table 22, **STP and RSTP Parameters** on page 230.
- 3. Click *Apply*.
Changes are immediately activated on the switch.

Configuring a Port's STP Settings

- To configure a port's STP settings, perform the following procedure:
- 1. From the STP Configuration Spanning Tree window in Figure 93 on page 233, click the Module pull-down menu and select the switch whose ports in the stack you want to configure.
 - 2. Click a port in the graphical switch image. You can select more than one port at a time.
A selected port turns white. (To deselect a port, click it again.)
 - 3. Click *Modify*.
- The STP Settings window displayed in Figure 94 is displayed.

STP Settings - Port(s) 6

Port Priority [0-15] 8 * 16 = 128	Path Cost [0 - 2000000000] 0 (0 = Auto Update)
---	--

Apply Cancel

Figure 94 STP Settings Window

- 4. Enter or modify the STP settings as desired.
For descriptions of the parameters, refer to Table 22, **STP and RSTP Parameters** on page 230.
- 5. Click *Apply*.

Note
A change to the port priority parameter takes effect immediately. A change to the port cost value requires you to reset the stack. A new port cost value is not implemented until the stack is reset.

Displaying STP Status and Settings

Displaying Bridge's STP Status and Settings

To display a bridge's STP status and settings, perform the following procedure:

1. From the Home page, select *Monitoring*.
2. From the Monitoring menu, select *Layer 2* tab.
3. From the Layer 2 window, select the *Spanning Tree* tab.

The Spanning Tree window in Figure 95 is displayed.

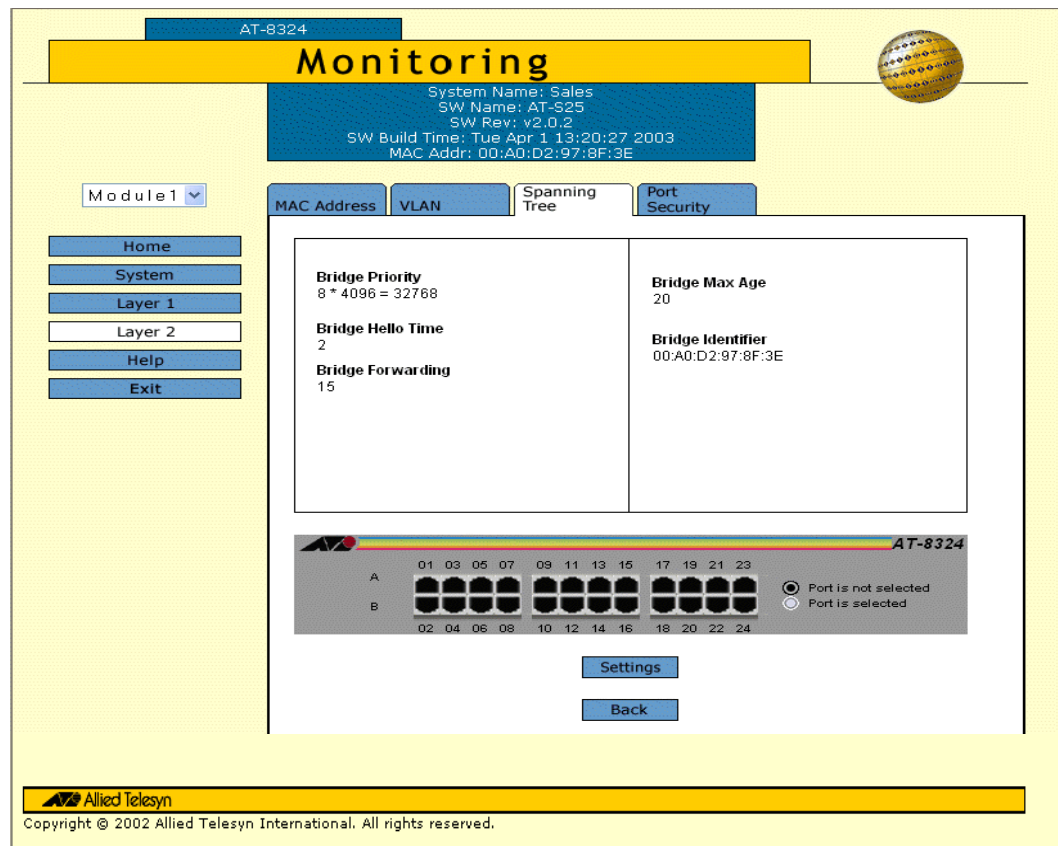


Figure 95 Monitoring - Spanning Tree Window

The parameters displayed in this window are for viewing purpose only. For description of these parameters, refer to Table 22, **STP and RSTP Parameters** on page 230.

Displaying Port's STP Status and Settings

To display the port's STP status or settings, perform the following procedure:

1. From the Spanning Tree window in Figure 95, select a port or a group of ports you wish to display the status or settings.

The selected port(s) will turn white. (To deselect a port, click it again.)

- 2. Click *Settings*, the STP Port Status window displayed in Figure 96 is displayed.

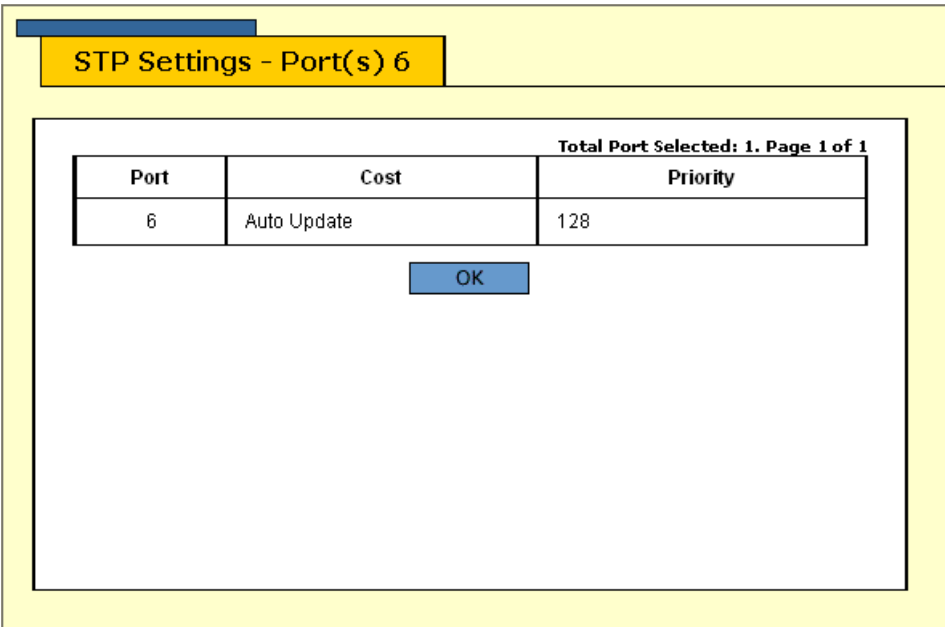


Figure 96 Monitoring - STP Settings Window

The port’s STP settings displayed in this window are for viewing purpose only. Refer to **Configuring a Port’s STP Settings** on page 234 for parameter descriptions.

Configuring RSTP

Configuring a Bridge's RSTP Settings

This section contains the procedure for configuring a bridge's RSTP settings.



Caution

The bridge provides default RSTP parameters that are adequate for most networks. Changing them without prior experience and an understanding of how RSTP works might have a negative effect on your network. You should consult the IEEE 802.1w standard before changing any of the RSTP parameters.

Considering that you have enabled RSTP as instructed in **Enabling or Disabling STP or RSTP** on page 228.

To configure RSTP, perform the following procedure:

1. From the Spanning Tree window, as displayed in Figure 92 on page 228, with SRTP Configuration as your selection.
2. Click *Configure*.

The RSTP Configuration Spanning Tree window in Figure 92 is displayed.

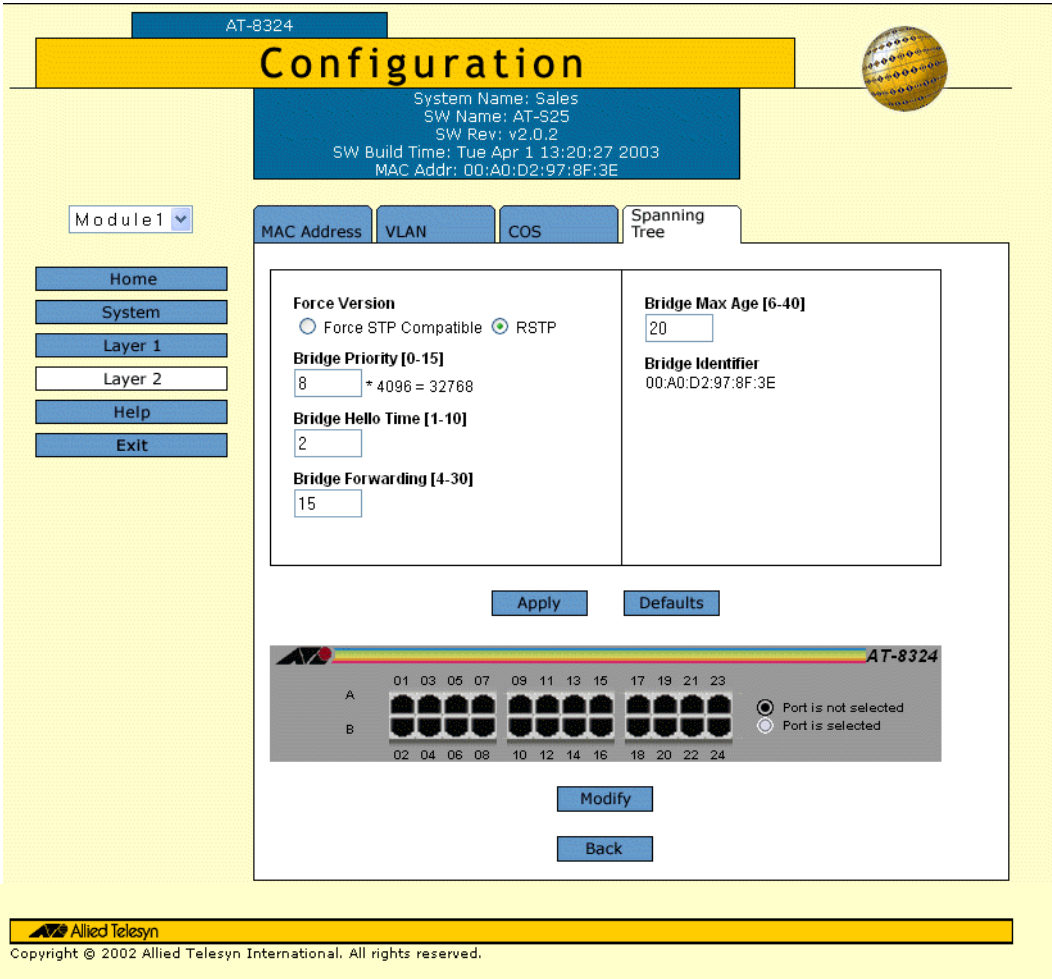


Figure 97 RSTP Configuration Spanning Tree Window

3. Enter or modify the RSTP configuration settings as desired.
For description of the parameters displayed in this window, refer to Table 22, **STP and RSTP Parameters** on page 230.
4. Click *Apply*.
Changes are immediately activated on the switch.

Configuring a Port's RSTP Settings

- To configure a port's RSTP settings, perform the following procedure:
1. From the RSTP Configuration Spanning Tree window, as displayed in Figure 93 on page 233, select a port.
A selected port turns white. (To deselect a port, click it again.)
 2. Click *Settings*.

The RSTP Settings window displayed in Figure 94 is displayed.

The image shows a software window titled "RSTP Settings - Port(s) 6". Inside the window, there are four settings sections arranged in a 2x2 grid:

- Port Priority [0-15]:** A text box containing the value "8", followed by the text "* 16 = 128".
- Path Cost [0 - 200000000]:** A text box containing the value "0", followed by the text "(0 = Auto Update)".
- Point-To-Point:** A dropdown menu currently showing "Auto Detect".
- Edge Port:** A dropdown menu currently showing "Yes".

At the bottom of the window, there are two buttons: "Apply" and "Cancel".

Figure 98 RSTP Settings Window

3. Enter or modify the RSTP settings as desired.

For description of the parameters in this window, refer to Table 22, **STP and RSTP Parameters** on page 230.

4. Click *Apply*.

Note

All changes to a port's RSTP settings, with the exception of port cost, are activated immediately. A change to the port cost value requires you to reset the switch. A new port cost value is not implemented until the unit is reset.

Displaying RSTP Status and Settings

Displaying Bridge's RSTP Status and Settings

To display a bridge's STP parameter status and settings, perform the following procedure:

1. From the Home page, select *Monitoring*.
2. From the Monitoring menu, select *Layer 2* tab.
3. From the Layer 2 window, select the *Spanning Tree* tab.

The Spanning Tree window in Figure 95 is displayed.

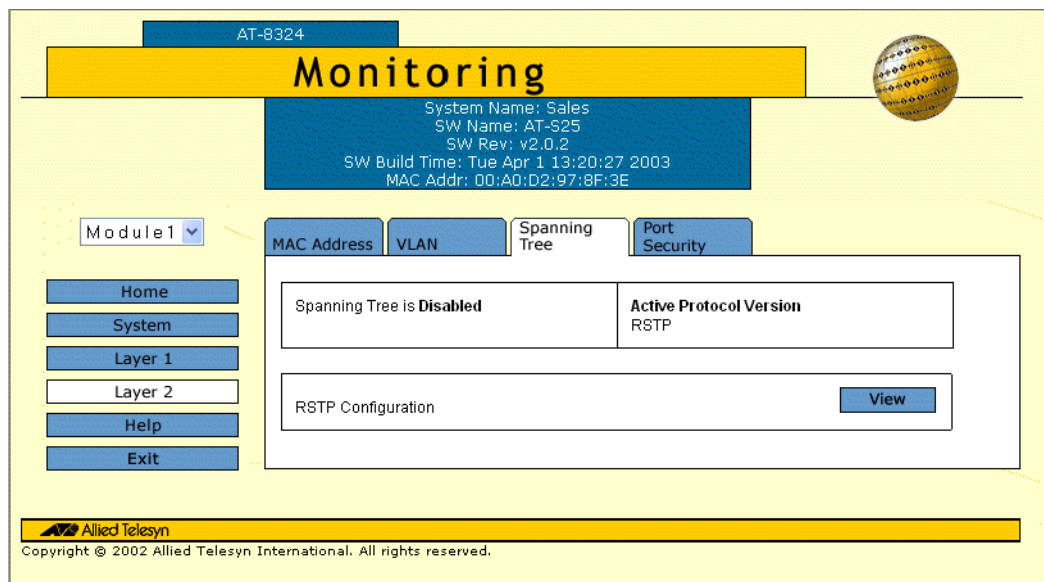


Figure 99 Monitoring - Spanning Tree Window

Displaying Port's RSTP Status and Settings

To display the port's RSTP status or settings, perform the following procedure:

1. From the graphical image of an AT-8324 Ethernet switch in the Spanning Tree window displayed in Figure 95; select a port or a group of ports you wish to display the status or settings.

The selected port(s) will turn white. (To deselect a port, click it again.)

- Click **Settings**, the RSTP Settings window displayed in Figure 100 is displayed.

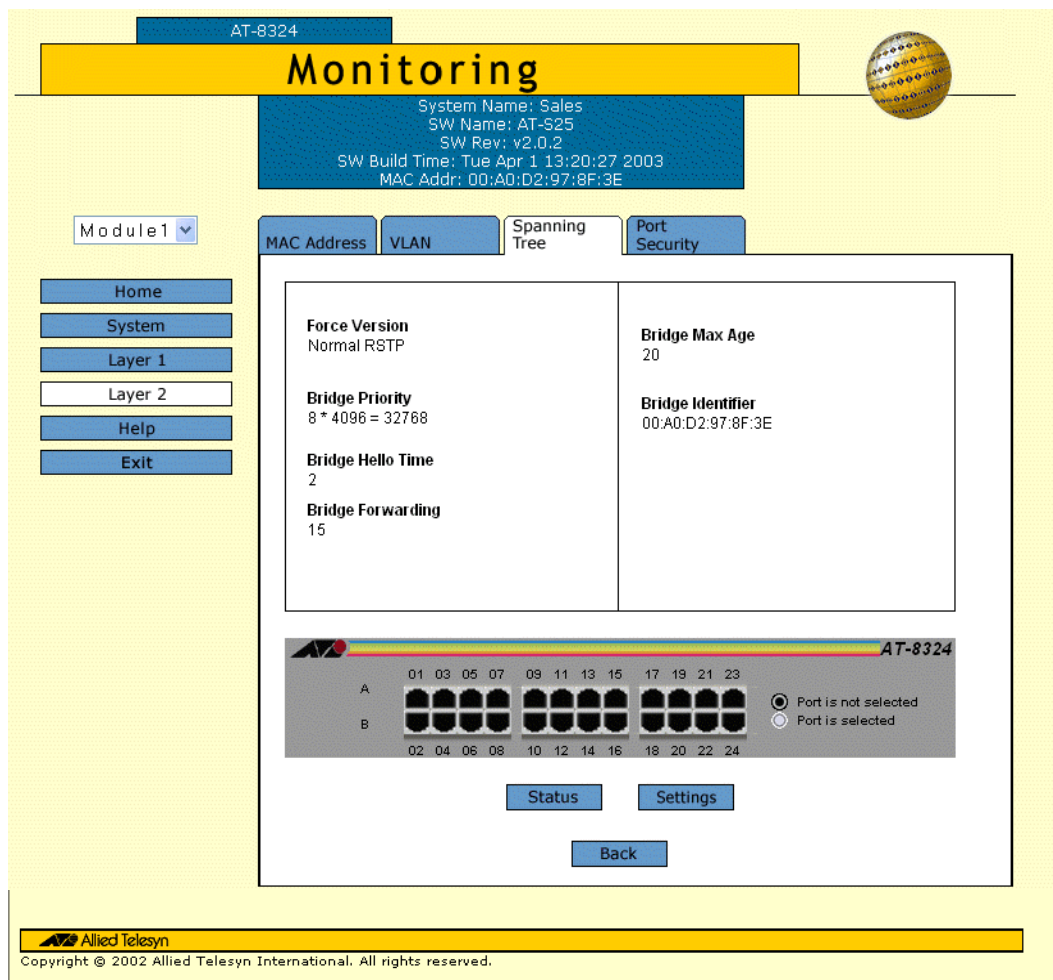


Figure 100 Monitoring - RSTP Settings Window

The parameters displayed in this window are for viewing purpose only. For description of these parameters, refer to Table 22, **STP and RSTP Parameters** on page 230.

Chapter 22

Virtual LANs

This chapter contains the procedure on how to create, modify, and delete VLANs from a web browser management session. This chapter also explains how to change a switch's VLAN operating mode.

Note

For background information on VLANs and the Basic VLAN mode, refer to **Chapter 10, Virtual LANs**.

This chapter contains the following sections:

- ❑ **Creating a VLAN** on page 243
- ❑ **Modifying a VLAN** on page 245
- ❑ **Deleting VLANs** on page 247
- ❑ **Displaying VLANs** on page 248
- ❑ **Changing a PVID Value** on page 250
- ❑ **Setting the Switch's VLAN Mode** on page 252

Creating a VLAN

To create a new VLAN, perform the following procedure:

1. From the Home page, select *Configuration*.
2. From the Configuration menu, select *Layer 2*.
3. From the Layer 2 window, select the *VLAN* tab.

The VLAN window in Figure 101 is displayed.

AT-8324

Configuration

System Name: Sales
SW Name: AT-S25
SW Rev: v2.0.2
SW Build Time: Tue Mar 25 15:20:05 2003
MAC Addr: 00:A0:D2:97:8F:3E

Home System Layer 1 Layer 2 Help Exit

MAC Address **VLAN** COS Spanning Tree

Name	VID	Name	VID
Default_VLAN	1		

Modify Remove Add Clear All

Allied Telesyn
Copyright © 2002 Allied Telesyn International. All rights reserved.

Figure 101 Configuration - VLAN Window

4. Click *Add*.

The Add New VLAN window in Figure 102 is displayed.

Add New VLAN

VID : 2

Name :

Module ID	Untagged Ports	Tagged Ports
1		
2		

Apply Cancel

Figure 102 Add VLAN Window

5. The AT-S25 management software automatically assigns the next unused VID in the stack as the VID for the new VLAN. To assign the VLAN a different VID, click the VID field and enter a new VID for the VLAN. The range is 2 to 2048. The VID must be unique from the other VLANs defined in the same stack.
6. Click the Name text field and enter a name for the new VLAN of from one to fifteen alphanumeric characters. The name should reflect the function of the nodes of the VLAN (for example, Sales or Accounting). The name can contain spaces, but not special characters, such as asterisks (*) or exclamation points (!). A VLAN must have a name.

A VLAN's name must be unique on the stack. You cannot assign the same name to two VLANs in the same stack.
7. To add tagged and untagged ports to the VLAN, specify the ports in the Untagged Ports and Tagged Ports fields next to each module. You can specify the ports individually (e.g., 2,5,11), as a range (e.g., 5-10), or both (e.g., 3,7,11-15,17).
8. Click *Apply*.

The new VLAN is now operational.

Repeat this procedure starting with Step 4 to create additional port-based and tagged VLANs.

Note

When you create a new VLAN, ports designated as untagged ports of the new VLAN are automatically removed from their current untagged VLAN assignment. For example, if you are creating a new VLAN on a switch that contains only the Default_VLAN, the ports that you specify as untagged ports of the new VLAN are automatically removed from the Default_VLAN when they are moved to the new VLAN.

Tagged ports are not removed from any current VLAN assignments because tagged ports can belong to more than one VLAN at a time.

Modifying a VLAN

To modify a port-based or tagged VLAN, perform the following procedure:

1. From the Home page, select *Configuration*.
2. From the Configuration menu, select *Layer 2*.
3. From the Layer 2 window, select the *VLAN* tab.

The VLAN window in Figure 101 on page 243 is displayed.

4. Click the button next to the name of the VLAN you want to modify.
5. Click *Modify*.

The View/Update VLAN configuration window is displayed in Figure 103.

Module ID	Untagged Ports	Tagged Ports
1	1-24	NONE
2	1-24	NONE

Figure 103 View/Update VLAN Window

Note

You cannot change the VID of a VLAN.

6. To change a VLAN's name, click the Name text field and enter the new name. A VLAN name can be from one to fifteen alphanumeric characters. The name should reflect the function of the nodes of the VLAN (for example, Sales or Accounting). The name can contain spaces, but not special characters, such as asterisks (*) or exclamation points (!). A VLAN must have a name.

A VLAN's name must be unique in the stack. You cannot assign the same name to two VLANs in the same stack.

7. To add or remove tagged and untagged ports from the VLAN, modify the Untagged Ports and Tagged Ports fields next to each module. You can specify the ports individually (e.g., 2,5,11), as a range (e.g., 5-10), or both (e.g., 3,7,11-15,17).

Note

Removing an untagged port from the Default_VLAN without assigning it to another VLAN will leave the port as an untagged member of no VLAN.

8. Click *Apply*.

Untagged ports that are added to a VLAN are automatically removed from their current VLAN assignment. Untagged ports that are removed from a VLAN are returned to the Default_VLAN.

The modified VLAN is now ready for network operations.

Deleting VLANs

To delete a VLAN from the switch, perform the following procedure:

1. From the Home page, select *Configuration*.
2. From the Configuration menu, select *Layer 2*.
3. From the Layer 2 window, select the *VLAN* tab.

The VLAN window in Figure 101 on page 243 is displayed.

4. Click the circle next to the name of the VLAN you want to delete.

Note

You cannot delete the Default_VLAN.

5. Click *Remove*.

A confirmation prompt is displayed.

6. Click *OK* to delete the VLAN or *Cancel* to cancel the procedure.

If you click OK, the VLAN is deleted from the switch. The untagged ports in the VLAN are returned to the Default_VLAN as untagged ports.

To delete all VLANs from the switch, perform the following procedure:

1. From the Home page, select *Configuration*.
2. From the Configuration menu, select *Layer 2*.
3. From the Layer 2 window, select the *VLAN* tab.

The VLAN tab window in Figure 101 on page 243 is displayed.

4. Click *Clear All*.

A confirmation prompt is displayed.

5. Click *OK* to delete all the VLANs or *Cancel* to cancel the procedure.

If you click OK, all VLANs except for the Default_VLAN are deleted from the switch. The ports in the VLANs are returned to the Default_VLAN as untagged ports.

Displaying VLANs

To display all the existing VLANs on a switch, perform the following procedure:

- 1. From the Home page, select *Monitoring*.
- 2. From the Monitoring page, select *Layer 2*.
- 3. From the Layer 2 page, select the *VLAN* tab.

The VLAN window in Figure 104 is displayed.

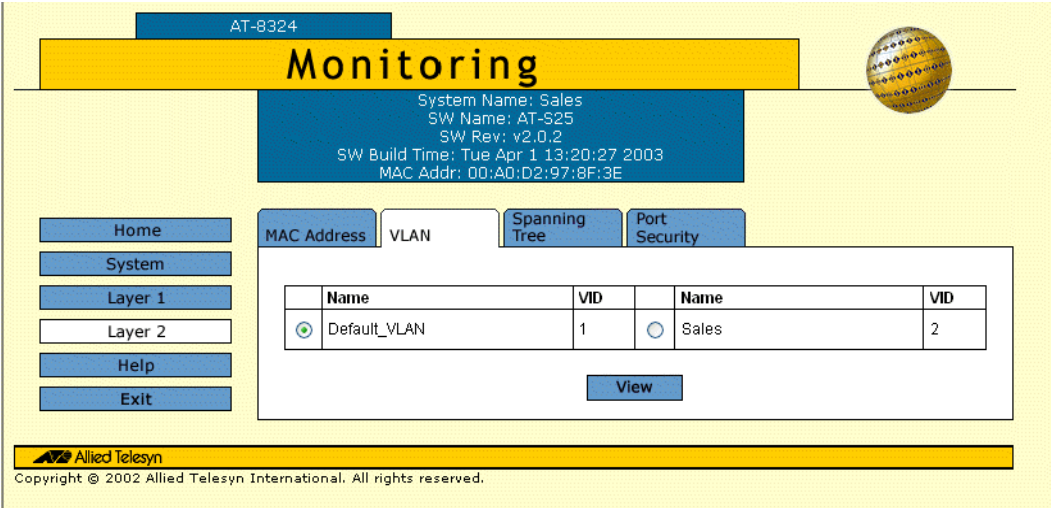


Figure 104 Monitoring - VLAN Window

- 4. Click the button next to the name of the VLAN you wish to view.
- 5. Click *View*.

The View VLAN window in Figure 105 is displayed.

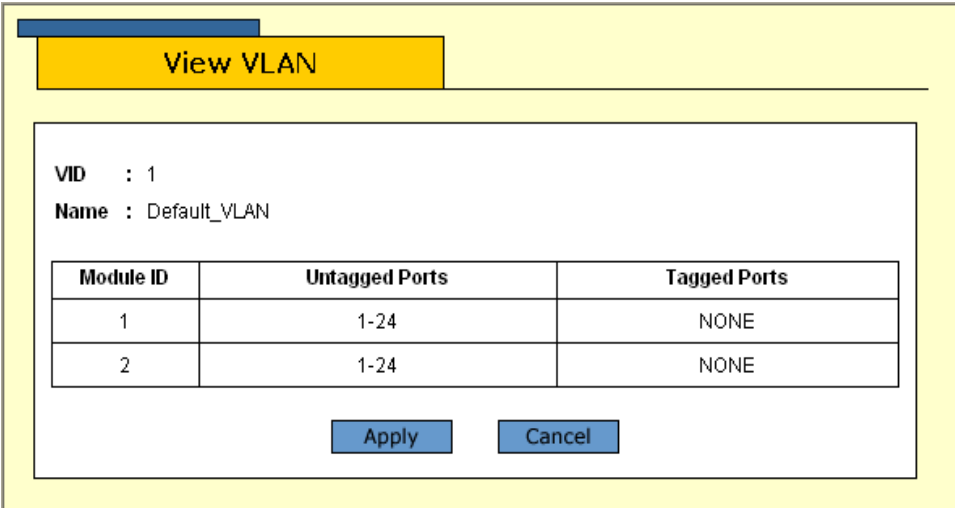


Figure 105 View VLAN Window

The parameters displayed in this window are for viewing purpose only. For information on these parameters, refer to **Creating a VLAN** on page 243.

6. Click *Cancel* to return to the previous menu.

Changing a PVID Value

The procedure in this section explains how to change a PVID value for a switch port. As explained in **Port-based VLAN Overview** on page 120, a port is assigned a PVID when it becomes an untagged port of a VLAN. A port's PVID will be the same as the VLAN's VID. For example, if you assign Port 4 on a switch as an untagged port to a VLAN with a VID of 7, the port is automatically assigned a PVID also of 7.

The assignment of PVIDs is performed automatically by the AT-S25 software. There should be little need for you to manually change this value. But the AT-S25 software does allow you to adjust the value if you find it necessary.

To change the PVID for a port, perform the following procedure:

1. From the Home page, select *Configuration*.
2. From the Configuration page, select *Layer 2*.
3. From the Layer 2 page, select the *COS* tab.

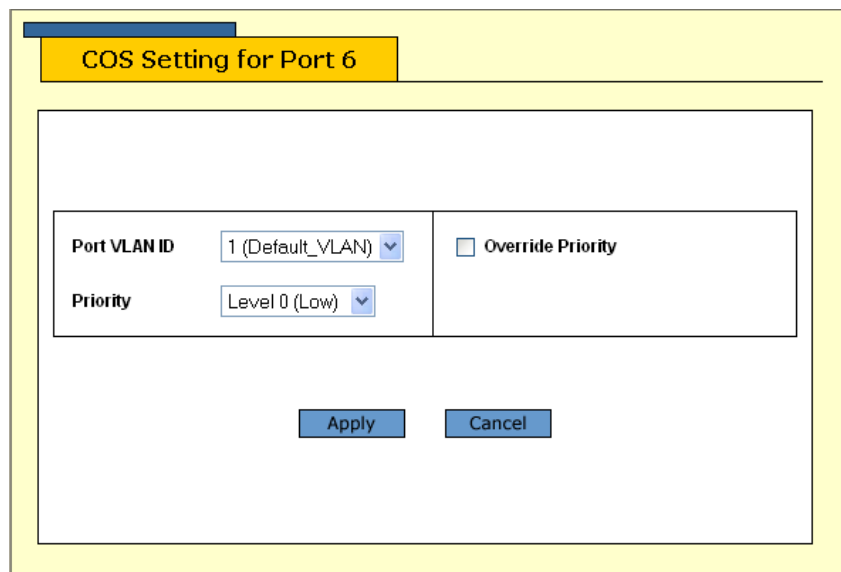
A graphical image of the AT-8300 Series switch is displayed.

4. Click the port whose PVID value you want to change. You can select only one port at a time.

A selected port turns white. (To deselect a port, click it again.)

5. Click *Modify*.

The COS Setting window in Figure 106 is displayed.



The image shows a web browser window titled "COS Setting for Port 6". Inside the window, there is a form with two rows of settings. The first row has a label "Port VLAN ID" followed by a dropdown menu showing "1 (Default_VLAN)" and a checkbox labeled "Override Priority" which is currently unchecked. The second row has a label "Priority" followed by a dropdown menu showing "Level 0 (Low)". At the bottom of the form, there are two buttons: "Apply" and "Cancel".

Figure 106 COS Setting Window

Note

The selections Priority and Priority Override are described in **Chapter 22, Class of Service** on page 262.

6. Click the Port PVID VID pull-down menu and select the new PVID value for the port.

The pull-down list displays the VIDs of all the existing VLANs in the stack. When you select a VID, the port's PVID is changed to match the selected VID.

7. Click *Apply*.

The change is immediately activated on the switch.

Setting the Switch's VLAN Mode

This section contains the procedure for setting a stack's VLAN mode. You can configure a stack to support port-based and tagged VLANs or to operate in the Basic VLAN mode. A stack can operate in only one VLAN mode at a time.

Note

Refer to **Chapter 10, Virtual LANs**, for background information on port-based and tagged VLANs and the Basic VLAN mode.

To set the stacks VLAN mode, perform the following procedure:

1. From the Home Page, select *Configuration*.

The Configuration window is displayed with the System menu option selected by default.

2. If the System menu option is not selected, select it.
3. Select the *General* tab.

The General tab window is displayed in Figure 107.

The screenshot shows the 'Configuration' window for a switch. The title bar indicates 'AT-8324'. The main header is 'Configuration'. Below it, system information is displayed: System Name: Sales, SW Name: AT-S25, SW Rev: v2.0.2, SW Build Time: Tue Mar 25 15:20:05 2003, MAC Addr: 00:A0:D2:97:8F:3E. The left sidebar contains navigation buttons: Home, System, Layer 1, Layer 2, Help, and Exit. The main content area has tabs for General, SNMP, IGMP, and Factory Default. The 'General' tab is active, showing three sections: Administration, Manager Password, and Configuration. The 'Administration' section includes fields for System Name (Sales), Administrator, Comments, IP Address (149.35.19.153), Subnet Mask (255.255.252.0), and Default Gateway (149.35.16.1). The 'Manager Password' section has fields for Manager Password, Confirm Manager Password, Operator Password, and Confirm Operator Password. The 'Configuration' section includes BOOTP/DHCP (Enable/Disable), MAC address aging time (300), and Switch Mode (Basic/Tagged). The 'Tagged' radio button is selected. At the bottom, there are 'Apply', 'Defaults', and 'Reset' buttons. The footer shows the Allied Telesyn logo and copyright information: Copyright © 2002 Allied Telesyn International. All rights reserved.

Figure 107 Configuration - General Window

4. In the Switch Mode section of the window, click either *Basic* or *Tagged*.
 - ☐ If you select Basic, the switch will operate in the Basic VLAN mode.
 - ☐ If you select Tagged, which is the default, the switch will support port-based VLANs and tagged VLANs.
5. Click *Apply*.
6. Click *Reset* to reset the stack.

Note

The new VLAN mode is not activated until the stack is reset.

Chapter 23

MAC Address Table

This chapter contains instructions on how to view the dynamic and static and multicast addresses in the MAC Address Table of the switch. This chapter contains the following procedure:

- ☐ **Viewing the MAC Address Table** on page 255
- ☐ **Adding Static and Multicast MAC Addresses** on page 258
- ☐ **Deleting MAC Addresses** on page 259
- ☐ **Changing the Aging Time** on page 260

Note

For background information on MAC addresses, refer to **MAC Address Overview** on page 147.

Viewing the MAC Address Table

To view the MAC Address Table, perform the following procedure:

1. From the Home page, select either *Configuration* or *Monitoring*.
2. From either the Configuration or the Monitoring page, select *Layer 2*.
3. From the Layer 2 page, select the *MAC Address* tab.

The MAC Address window Figure 108 is displayed.

Figure 108 MAC Address Window

Table 23 lists the parameters appeared in the MAC Address window.

Table 23 MAC Address Parameters

PARAMETER	DESCRIPTION
View All MAC Addresses	View all the MAC addresses that have been assigned to the module.
View All Static Addresses	View all the static MAC addresses that have been assigned to the module.
View by Module	View the MAC addresses that have been assigned to the selected module.

PARAMETER	DESCRIPTION
View all multicast MAC addresses	View all the multicast MAC addresses that have been assigned to the module.
View by Module & Port	View any MAC addresses that have been assigned to a particular module and port.
View by VLAN ID	View any MAC addresses that have been assigned to a VLAN ID.
View Port & Module number of MAC Address	View the port, module number, and VLAN ID where a MAC Address is assigned to.

4. Once you have selected one of the options, click *View*.

The MAC Address Table in Figure 109 is displayed.

MAC Address Table					
Page 1					
	MAC ADDRESS	MODULE	PORT	VLAN ID	TYPE
<input type="radio"/>	0000CD 00E51F	01	6	01	Dynamic
<input type="radio"/>	0000CD 016B5D	01	6	01	Dynamic
<input checked="" type="radio"/>	0000F4 A41244	01	6	01	Dynamic
<input type="radio"/>	0000F4 DD2931	01	6	01	Dynamic
<input type="radio"/>	00065B 3C5F1E	01	6	01	Dynamic
<input type="radio"/>	00065B 7929DD	01	6	01	Dynamic
<input type="radio"/>	00065B 890704	01	6	01	Dynamic
<input type="radio"/>	00065B A367D6	01	6	01	Dynamic
<input type="button" value="Refresh"/> <input type="button" value="Remove"/> <input type="button" value="Next"/> <input type="button" value="Close"/>					

Figure 109 Example of MAC Address Table

Table 23 lists the parameters appeared in the MAC Address Table.

Table 24 MAC Address Table Parameters

PARAMETER	DESCRIPTION
MAC ADDRESS	The MAC address of the node connected to the switch.
MODULE	The selected module.
PORT	The port on the switch where the MAC address was learned.

PARAMETER	DESCRIPTION
VLAN ID	The VID of the VLAN to which the port is an untagged member.
TYPE	The MAC address type. The type can be either static or dynamic.

Adding Static and Multicast MAC Addresses

This section contains the procedure for assigning static address to the ports on the switch. You could assign up to 255 static MAC addresses per port.

To add a static address to the MAC Menu, perform the following procedure:

1. From the Home page, select *Configuration*.
2. From the Configuration page, select *Layer 2*.
3. From the Layer 2 page, select the *MAC Address* tab.

The MAC Address window in Figure 108 on page 255 is displayed.

4. Click *Add*.

The Add Static MAC Address window in Figure 110 is displayed.

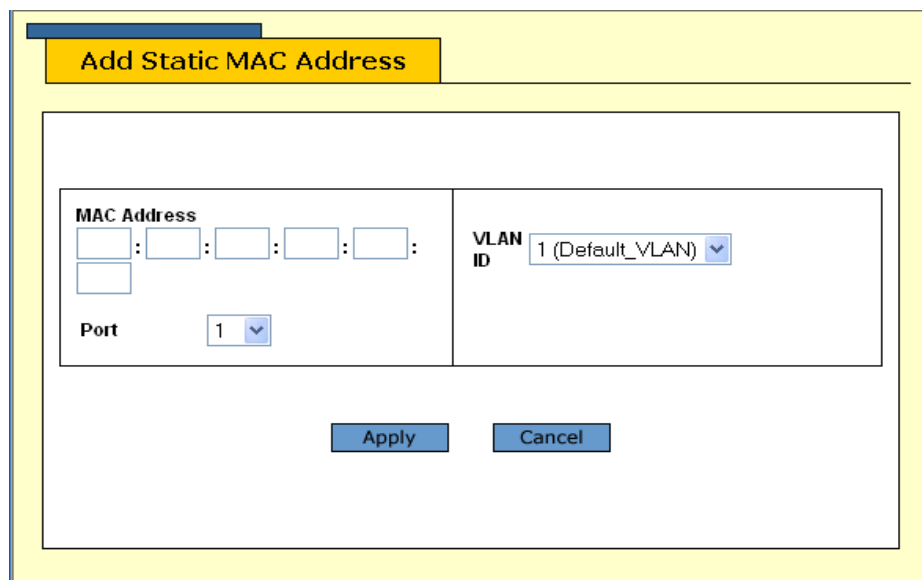
The image shows a web browser window titled "Add Static MAC Address". The window has a yellow header bar with the title. Below the header is a white content area. On the left side of the content area, there is a section labeled "MAC Address" with five input fields for the MAC address (XX:XX:XX:XX:XX:XX) and a "Port" dropdown menu currently showing "1". On the right side, there is a "VLAN ID" dropdown menu currently showing "1 (Default_VLAN)". At the bottom of the content area, there are two buttons: "Apply" and "Cancel".

Figure 110 Add Static MAC Address window

5. In the MAC Address section of the window, enter the new static MAC address.
6. Select a port and a VLAN ID.
7. Click *Apply*.
8. Repeat this procedure to add other static addresses to the switch.

Deleting MAC Addresses

To delete a static, dynamic, or multicast MAC address from the switch, perform the following procedure:

1. From the Home page, select *Configuration*.
2. From the Configuration page, select *Layer 2*.
3. From the Layer 2 page, select the *MAC Address* tab.

The MAC Address window in Figure 108 on page 255 is displayed.

4. Display the MAC addresses on the switch by selecting one of the options. For instructions, refer to **Viewing the MAC Address Table** on page 255.
5. Click on the button next to the MAC address that you wish deleted from the switch.
6. Click *Remove*.

Changing the Aging Time

The switch uses the aging time to delete inactive dynamic MAC addresses from the MAC Menu. When the switch detects that no packets have been sent to or received from a particular MAC address in the table after the period specified by the aging time, the switch deletes the address. This prevents the table from becoming full of addresses of nodes that are no longer active.

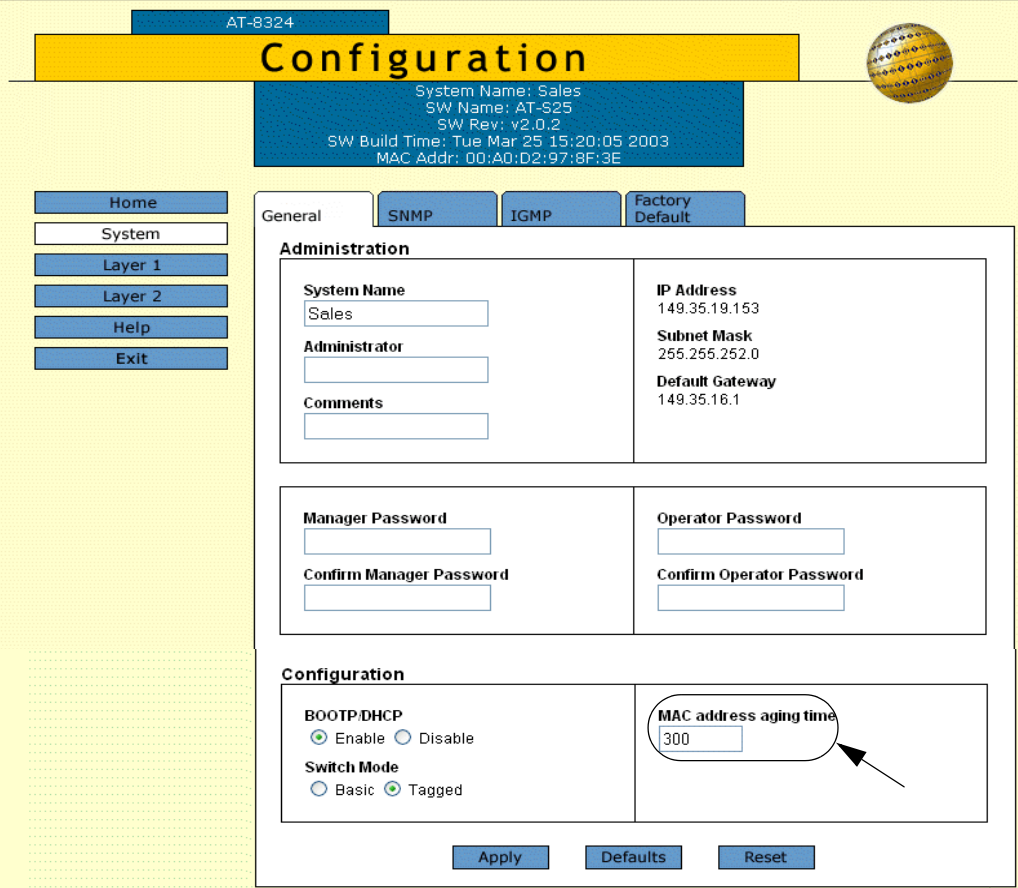
To adjust the aging time, perform the following procedure:

1. From the Home page, select *Configuration*.

The Configuration window is displayed with the System menu option selected by default.

2. If the System menu option is not selected, select it and then select the *General* tab.

The General window in Figure 111 is displayed.



AT-8324

Configuration

System Name: Sales
SW Name: AT-S25
SW Rev: v2.0.2
SW Build Time: Tue Mar 25 15:20:05 2003
MAC Addr: 00:A0:D2:97:8F:3E

Home System Layer 1 Layer 2 Help Exit

General SNMP IGMP Factory Default

Administration

System Name Sales	IP Address 149.35.19.153
Administrator	Subnet Mask 255.255.252.0
Comments	Default Gateway 149.35.16.1

Manager Password	Operator Password
Confirm Manager Password	Confirm Operator Password

Configuration

BOOTP/DHCP <input checked="" type="radio"/> Enable <input type="radio"/> Disable Switch Mode <input type="radio"/> Basic <input checked="" type="radio"/> Tagged	MAC address aging time 300
---	-------------------------------

Apply Defaults Reset

Allied Telesyn
Copyright © 2002 Allied Telesyn International. All rights reserved.

Figure 111 Configuration - General Window

3. In the MAC address aging time text box, enter the new value in seconds. The default setting for the aging time is 300 seconds (5 minutes).
4. Click *Apply* to accept the new value of the MAC address aging time.

Chapter 24

Class of Service

This chapter contains instructions on how to configure CoS. This chapter contains the following procedure:

- ❑ **Configuring CoS** on page 263

Note

For background information on CoS, refer to **Class of Service Overview** on page 162.

Configuring CoS

To configure CoS, perform the following procedure:

1. From the Home page, select *Configuration*.
2. From the Configuration page, select *Layer 2*.
3. From the Layer 2 page, select the *COS* tab.

A graphical image of an AT-8316F or an AT-8324 Fast Ethernet Switch is displayed.

4. Click the port where you wish to configure the CoS.

You could select only one port at a time. A selected port turns white. (To deselect a port, click it again.)

5. Click *Modify*.

The COS Setting window in Figure 112 is displayed.

Figure 112 COS Setting Window

6. Click the Priority pull-down menu and select either the high or low priority queue for the port. The default is the low priority queue.
7. Select the Override Priority check box if you are configuring a tagged port and you wish the switch to ignore the priority tag in the tagged frames entering the port.

The default for this parameter is No, meaning that the priority level of tagged frames is determined by the priority level specified in the frame itself.

Table 25 lists the parameters appeared in the COS Setting window.

Table 25 COS Setting Parameters

PARAMETER	DESCRIPTION
Port VLAN ID	Select the port VLAN ID.
Priority	<p>Specify which priority level queue all tagged and untagged frames received on the port go to.</p> <p>Possible settings for this parameter are:</p> <ul style="list-style-type: none">• Level 0 (Low) - Low priority queue.• Level 1 (High) - High priority queue
Override Priority	<p>Select this check box if you are configuring a tagged port and you wish the switch to ignore the priority tag in the tagged frames entering the port.</p> <p>The default for this parameter is No, meaning that the priority level of tagged frames is determined by the priority level specified in the frame itself.</p>

Note

The tagged information in a frame is not changed as the frame traverses the switch. A tagged frame exits the switch with the same priority level that it had when it entered.

8. Click *Apply*.

Changes are immediately activated on the switch.

Chapter 25

IGMP Snooping

This chapter describes how to configure the IGMP snooping feature on the stack.

Note

For background information on this feature, refer to **IGMP Snooping Overview** on page 167.

Sections in the chapter include:

- ❑ **Configuring IGMP Snooping** on page 266
- ❑ **Displaying a List of Host Nodes and Multicast Routers** on page 269

Configuring IGMP Snooping

To configure IGMP snooping from a web browser management interface, perform the following procedure:

1. From the Home page, select *Configuration*.

The Configuration window is displayed with the System menu option selected by default.

2. If the System menu option is not selected, select it and then select the *IGMP* tab.

The IGMP window in Figure 113 is displayed.

Figure 113 Configuration - IGMP Window

3. Adjust the IGMP parameters as necessary.

The parameters are described below:

PARAMETER	DESCRIPTION
Enable IGMP Snooping Status	Enables and disables IGMP snooping on the stack. A check in the box indicates that IGMP is enabled.

PARAMATER	DESCRIPTION
Multicast Host Topology	<p>Defines whether there is only one host node per stack port or multiple host nodes per port.</p> <p>Possible settings for this parameter are:</p> <ul style="list-style-type: none"> • Single-Host/Port (Edge) is appropriate when there is only one host node connected to each port on the stack. This setting causes the stack to immediately stop sending multicast packets out a stack port when a host node signals its desire to leave a multicast group by sending a leave request or when the host node stops sending reports and times-out. The stack forwards the leave request to the router and simultaneously ceases transmission of any further multicast packets out the port where the host node is connected. • (Multi-Hosts/Port (Intermediate) is appropriate if there is more than one host node connected to a stack port, such as when a port is connected to an Ethernet hub to which multiple host nodes are connected. With this setting selected the stack continues sending multicast packets out a port even after it receives a leave request from a host node on the port. This ensures that the remaining active host nodes on the port will continue to receive the multicast packets. Only after all of the host nodes connected to a stack port have transmitted leave requests (or have timed out) will the stack stop sending multicast packets out the port. <p>If a stack has a mixture of host nodes, that is, some connected directly to the stack and others through an Ethernet hub, you should select the Intermediate Multi-Host Port selection.</p>
Host/Router Timeout Interval	<p>Specifies the time period in seconds after which the stack determines that a host node has become inactive. An inactive host node is a node that has not sent an IGMP report during the specified time interval. The range is from 1 second to 86,400 seconds (24 hours). The default is 260 seconds.</p> <p>This parameter also specifies the time interval used by the stack in determining whether a multicast router is still active. The stack makes the determination by watching for queries from the router. If the stack does not detect any queries from a multicast router during the specified time interval, it assumes that the router is no longer active on the port.</p>

PARAMATER	DESCRIPTION
Maximum Multicast Groups	<p>Specifies the maximum number of multicast groups the stack will learn. The range is 1 to 2048 groups. The default is 255 multicast groups.</p> <p>This parameter is useful with networks that contain a large number of multicast groups. You could use the parameter to prevent the stack's MAC Address Table from filling up with multicast addresses, leaving no room for dynamic or static MAC addresses. The range is 1 address to 2048 addresses. The default is 255 multicast addresses.</p>

4. Click *Apply*.

Changes are immediately activated on the stack.

Displaying a List of Host Nodes and Multicast Routers

You could use the AT-S25 software to display a list of the multicast groups on a stack, as well as the host nodes. You could also view the multicast routers. A multicast router is a router that is receiving multicast packets from a multicast application and transmitting the packets to host nodes. To view host nodes and multicast routers, perform the following procedure:

1. From the Home Page, select *Monitoring*.

The Monitoring window is displayed with the System menu option selected by default.

2. If the System menu option is not selected, select it and then select the *IGMP* tab.

The IGMP window in Figure 114 is displayed.

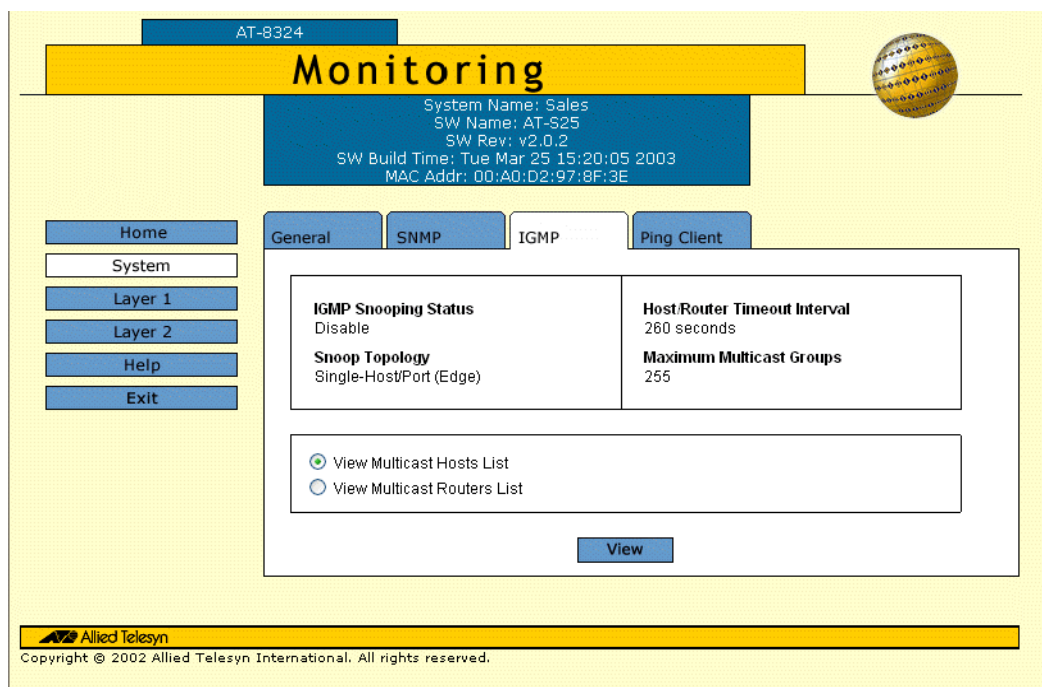


Figure 114 Monitoring - IGMP Window

The IGMP parameters displayed in this window are for viewing purpose only. For information on these parameters, refer to **Configuring IGMP Snooping** on page 266.

3. To view the multicast addresses and the host nodes, click *View Multicast Hosts List* and then click *View*.

The View Multicast Hosts List window in Figure 115 is displayed.

View Multicast Hosts List

Total Multicast Group: 0. Page 1 of 1

Multicast Group	VLAN ID	Module	Member Port	Host IP	Joined/Left

Refresh OK

Figure 115 View Multicast Hosts List Window

Table 26 lists the parameters appeared in the Multicast Hosts List window. These parameters are for viewing purposes only.

Table 26 View Multicast Hosts List Parameters

PARAMATER	DESCRIPTION
Multicast Group	The multicast address of the group.
VLAN ID	The VID of the VLAN in which the port is an untagged member.
Module	The selected module.
Member Port	The port(s) on the stack to which one or more host nodes of the multicast group are connected.
Host IP	The IP address(es) of the host node(s) connected to the port.
Joined/Left	<p>This parameter specified when a host node of the multicast group is connected or disconnected from the port.</p> <ul style="list-style-type: none"> • Joined is when the host node is connected to the port. • Left is when the host node is disconnected from the port. <p>So, for a host node participates in the group, it is displayed as "Joined", but whenever the host is no longer part of the multicast group, that field will be displayed as "Left" for a few minutes, until the next time interval the IGMP checks for host participation.</p>

4. To view the multicast routers, click *View Multicast Routers List* and then click *View*.

The View Multicast Routers List window in Figure 116 is displayed.

View Multicast Routers List

Total Multicast Router: 0. Page 1 of 1

Module	Port	VLAN Id	Router IP

Refresh OK

Figure 116 View Multicast Routers List Window

Table 27 lists the parameters appeared in the View Multicast Routers List window. These parameters are for viewing purposes only.

Table 27 View Multicast Routers List Parameters

PARAMATER	DESCRIPTION
Module	The selected module.
Port	The port(s) on the stack to which one or more host nodes of the multicast group are connected.
VLAN ID	The VID of the VLAN in which the port is an untagged member.
Router IP	The IP address(es) of the host node(s) connected to the port.

Appendix A

AT-S25 Default Settings

This appendix lists the AT-S25 factory default settings.

Settings	Default
IP Address	0.0.0.0
Subnet Mask	255.255.0.0
Gateway Address	0.0.0.0
System Name	None
MAC Aging Time	300 seconds
Community Strings	
Get Community String	public
Set Community String	private
Trap Community String	public
Spanning Tree Protocol and Rapid Spanning Tree Protocol	
Status	Disabled
Bridge Priority	Increment 8 (32768)
Bridge Max Age Time	20
Bridge Hello Time	2
Port Costs	Auto detect 2 000 000 - 10 Mbps 200 000 - 100 Mbps 20 000 - 1000 Mbps
Port Priority	Increment 8 (128)
Point-to-Point	Auto Detect
Edge Port	Yes

Settings	Default
IGMP Snooping	
Status	Disabled
Topology	Single Host/ Port (Edge)
Host/Router Time-out Interval	260 seconds
Maximum Multicast Groups	255
Management Interface	
Manager Login Name (web browser interface only)	manager
Manager Password	friend (case sensitive)
Operator Login Name (web browser interface only)	operator
Operator Password	operator (case sensitive)
Time Out Value	10 minutes
Twisted Pair Ports	
Status	Enabled
Duplex Mode	Auto-negotiation
Speed	Auto-negotiation
Flow Control	Disabled
Broadcast Packets	Forwarded
Security	Automatic
VLANs	
Default VLAN Name	Default_VLAN (all ports)
VID	1
Basic VLAN Mode	Disabled
Management Access	
Telnet	Enabled
SNMP	Disabled
TFTP	Enabled
RS-232 Port	
Data Bits	8
Stop Bits	1
Parity	None
Flow Control	Full-duplex
Data Rate	9600 bps

Index

A

- aging time
 - changing, 160, 260
 - defined, 148
- AT-8316F/MT Ethernet switch
 - port groups, 69, 79
- AT-8324 Ethernet switch
 - port groups, 69, 79
- AT-S25 default settings, 56, 205, 272
- AT-S25 software security, 50
- AT-S25 software updates
 - downloading from a local session, 17, 181, 186
- AT-S25 version number, 58
- Automatic port security level, 68
- Auto-Negotiation, 209

B

- Basic VLAN mode
 - defined, 129
 - setting, 252
- bootloader version number, 58
- BOOTP
 - activating, 17, 46, 198
 - defined, 46
- bridge identifier, 94
- bridge priority, 94
- browser tools, 192

C

- Class of Service
 - configuring, 163, 263
 - defined, 162
- console timeout, 50

D

- default values, AT-S25, 56, 205, 272
- DHCP

- activating, 17, 46, 198
- defined, 46

- document conventions, 14
- documentation, 16

F

- forwarding delay, 97

G

- gateway address, 43, 196
- guidelines, port trunking, 78

H

- hello time, 97
- host nodes
 - defined, 167
 - displaying, 172, 269
- host/router timeout interval, 171, 267

I

- IEEE 802.1d standard, 105
- IEEE 802.1w standard, 110, 233, 237
- IGMP snooping
 - configuring, 169, 266
 - defined, 167
- Internet Protocol (IP) address 42
- Internet Protocol (IP) address, 43, 195

L

- limited security mode
 - defined, 68
- local management interface
 - defined, 28
 - quitting, 37
- Lock All Ports security level, 71

M

MAC address table, 146, 255
 management access levels, 51
 Management Information Base (MIB), 31
 management VLAN, 143
 Manager access, 51
 Manager password, 51
 MIBs, supported, 31
 multicast groups, maximum, 171, 268
 multicast MAC address
 adding, 159, 258
 deleting, 157, 259
 multicast router, displaying, 173, 269

O

Operator access, 51
 Operator password, 51

P

password
 changing, 44, 196
 default, 36, 38, 50, 190
 pinging, 49, 204
 port
 configuring parameters, 60, 207
 disable, 209
 displaying status, 210
 speed, 62
 statistics, 175, 213
 port cost
 defined, 95
 setting, 103, 231
 port groups, 79
 port mirroring
 creating, 90, 223, 225
 defined, 89
 deleting, 223, 225
 port security
 configuring, 75
 defined, 68
 displaying, 215
 port trunking
 creating, 82, 83, 217, 219, 220
 defined, 78
 deleting, 85, 86, 87, 217, 219, 220
 guidelines, 78
 port VLAN identifier (PVID)
 changing, 250
 defined, 121, 126
 port VLAN identifier (VID), 121
 port-based VLAN
 creating, 130, 243
 defined, 120
 deleting all, 140
 deleting, 138, 247

displaying, 137, 248
 modifying, 134, 245
 priority queues, 162

Q

quitting
 local interface, 37
 Telnet interface, 39
 web browser interface, 192

R

Rapid Spanning Tree Protocol
 configuring port parameters, 111, 234, 238
 resetting a switch, 48, 199
 root bridge, 94
 RS232 port, default settings, 36

S

Secure level, port security, 70
 SNMP community strings, 54
 SNMP management interface, 31, 50
 snoop topology, 170, 267
 software updates
 downloading from a local session, 17, 181, 186
 Spanning Tree Protocol
 configuring bridge parameters, 105, 110, 233, 237
 configuring port parameters, 107
 defined, 93
 port cost, 95, 103, 231
 viewing bridge parameters, 235, 240
 starting interface
 Telnet, 38
 web browser, 190
 static MAC address
 adding, 159, 258
 deleting, 157, 259
 statistics
 port, 175, 213
 switch, 177
 STP. See Spanning Tree Protocol
 subnet mask, 43, 195
 switch statistics, 177
 system name, 43

T

tagged VLAN
 creating, 130, 243
 defined, 125
 deleting all, 140
 deleting, 138, 247
 displaying, 137, 248
 example, 127
 modifying, 134, 245

Index

Telnet management interface

- defined, 29
- quitting, 39
- starting, 38

TFTP, downloading and uploading files, 17, 181, 186

To 64

U

user name, default, 36, 38, 50, 190

V

version number, AT-S25, 58

virtual LAN

- creating, 130, 243
- defined, 118
- deleting all, 140
- deleting, 138, 247
- displaying, 137, 248
- mode, changing, 252
- modifying, 134, 245
- port-based, defined, 120
- tagged, defined, 125

VLAN. See virtual LAN

W

web browser management interface

- defined, 30
- limitations, 30
- quitting, 192
- starting, 190

web browser management session

- disabling, 50